Wireless Information Technology for the 21st Century

Information Technology Laboratory

National Institute of Standards and Technology

Authors: **Robert Glenn, Jan Erik Hakegard, Wayne Jansen, Tom Karygiannis, Sri Kumar, Donald Marks, Michael Miller, Kevin Mills, Nader Moayeri, and Madhavi Subbarao**

Status - From the Editor (Mills)

The authors have reviewed the draft material twice. The authors have also reviewed the projections, market inhibitors, and recommendations. At this time, the draft can be considered a consensus view among the authors.

Table of Contents

I. Introduction

In the 1960's voice communication was carried to end subscribers almost exclusively on copper wires running from central office switches to homes and businesses, and television was broadcast to homes almost exclusively through the air modulated on electromagnetic waves. By the late 1980's, industry pundits began to observe that the situation was reversing itself. Increasingly, voice communication was carried to end subscribers through the air modulated on electromagnetic waves, while television was broadcast to homes on copper coaxial cables (soon to be followed by fiber optic cables). Now, as the 21st century approaches, the situation appears decidedly more complex. Cellular telephony continues to expand at a rapid rate; however, numerous plans exist for high-speed wireless backbones carried across networks of earth-orbiting satellites, both geostationary and non-stationary, as well as networks of aircraft and balloons. In addition, several companies are devising plans to deploy broadband wireless distribution systems in order to compete with cable and copper twisted pairs for delivering high bandwidth data and television signals to businesses and homes. Further a variety of embedded and portable devices are beginning to appear, carrying built-in pico-cellular wireless communication transceivers. Two things appear clear. First, during the 21st century, wireless information technology will play a large role in the life of the country's citizens and in the country's economy. Second, the wireless technology landscape is so vast and complex that any organization seeking to enter the fray must take careful stock of the opportunities ahead.

This white paper, on wireless information technology for the 21st century, aims to inform the strategic decision-making process within the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). The paper surveys the vast landscape of wireless information technology. In doing so, the paper attempts: (1) to identify market inhibitors facing various wireless technologies, (2) to make projections about the likely road ahead, and (3) to seek opportunities for the ITL particularly, and NIST more generally, to contribute to the removal of market inhibitors for key wireless technologies. At the end, this white paper makes some recommendations on actions that the ITL and NIST should take to address the technological needs of the nascent wireless information technology industry. These needs include sharing the risk of development for key technical innovations and infrastructure standards, and providing the measurement science needed to inform industry decision-making when choosing among competing technical approaches to solve the difficult engineering problems inhibiting the successful deployment of wireless information technology.

II. Wireless Communications Systems

The market for wireless cellular telephony services has grown dramatically over the past 15 years, as wireless technology supporting such services has developed through two generations. At present, the wireless telephony industry is poised to develop and deploy a third generation of wireless systems that will increase spectral efficiency for voice users and offer flexible multimedia data services. The subsections that follow outline the progress of wireless telephony across all three generations, concentrating on the technical, economics, and standards battles raging with respect to the third-generation systems, which have yet to be deployed. The future of wireless communications technology is considered in order to identify opportunities for NIST to help the industry realize its technical and economic promise. The section closes with a consideration of opportunities for NIST to influence the future course of wireless communications, which will surely be a growth industry in the 21st century.

II.A 1st Generation Wireless Systems

The commercial use of mobile phones started in the US when AT&T developed the AMPS (Advanced Mobile Phone System) system in late 1970's [3GW9, 3GW1]. AMPS went into service first in Chicago area in 1983. The AMPS system is an analog communication system, which uses frequency modulation (FM) to transmit speech and frequency shift keying (FSK) to transmit important network control information in digital form [3GW10]. The AMPS system was designed primarily for carrying two-way voice conversations. Surprisingly, AMPS remains in use almost sixteen years after its introduction into the market. In fact, AMPS still enjoys 11% share of the cellular communications market in the US. Other analog mobile systems were introduced in Europe and Japan a few years earlier than AMPS was deployed in the US [3GW11]. However, unlike in the US, where AMPS was the only system introduced, European countries developed several incompatible systems. Lack of interoperability soon proved to be a major problem for many European users who regularly traveled to other countries within Europe for business and pleasure. The number of cellular users and the geographic coverage of the system increased steadily, but modestly, in the US.

II.B 2nd Generation Wireless Systems

In the 1980's the Europeans recognized the need for a second generation of cellular systems based on digital modulation and transmission schemes, which promised a more efficient use of the available frequency spectrum. This translates into increased total communication capacity and hence the capability to offer cellular service to a larger number of users per unit area. To avoid the interoperability problems encountered with the first-generation systems, the European countries agreed to jointly develop a common system for the entire continent. The result was the Global System for Mobile Communications (GSM), which was first commercially deployed in 1991 [3GW12, 3GW2]. GSM uses many features made possible by adoption of digital technology, such as digital voice compression and encryption. GSM also introduced many innovations in network level architectures and services. The multiple access mechanism in GSM is Time Division Multiple Access (TDMA), where each user in a cell transmits and receives information in time slots allocated to that user. The multiple access mechanism in the first-generation systems is Frequency Division Multiple Access (FDMA), where each user is allocated two bands or channels in the frequency spectrum, one for transmitting information and one for receiving it. GSM was a major success for Europe by all accounts, allowing users to roam all over the continent and yet be able to use their mobile phones. The success of GSM spread throughout the world. GSM now has the largest share of the market in the world with 64% of the user population using it [3GW2]. This was followed by the development of the digital cellular IS-54 standard [3GW13] in the US, which incorporated several important GSM network control innovations [3GW10].

The Japanese digital cellular standard, referred to as Pacific Digital Cellular (PDC), was designed soon after IS-54 was published [3GW14]. However, the Japanese soon found themselves with a system incompatible with AMPS, GSM, and IS-54. This system never found market acceptance outside of Japan.

During the almost ten-year development period of GSM in Europe, the Americans were reasonably satisfied with AMPS and there was no dire need for developing a new generation of mobile phones. This gradually changed when the number of users increased to a point where the AMPS system was no longer capable of providing the needed capacity. Of course, one can increase the capacity to a certain extent by making the cells smaller and having a larger frequency reuse. This was only a temporary solution and it soon became clear that a second-generation system had to be developed. This was the beginning of a lively, fierce, and often controversial debate on the access mode for the new system. A digital transmission technology called spread spectrum communications, developed for the US military more than 40 years ago [3GW15], was at the center of these discussions [3GW3]. In a spread spectrum system, a user spreads its transmitted signal over a frequency band much wider than the actual symbol bandwidth. This makes the signal look like noise, making eavesdropping difficult. The intended receiver, having knowledge of the spreading code or the frequency-hopping pattern used, is able to demodulate the signal. The privacy and security of spread spectrum communications makes it suitable for military communications.

As far as commercial use is concerned, spread spectrum is used with a multiple access scheme called Code Division Multiple Access (CDMA) [3GW15, 3GW16], where each transmitting user spreads its signal over the entire available spectrum using its individual code. This turns out to be a very flexible and efficient use of the frequency spectrum, where the users can come and go any time into the system and only slightly change the "noise level" as far as the other users are concerned. In addition, the spread spectrum system very naturally exploits the fact that speech consists of almost 40% silence, where there is nothing to be transmitted. This statistical multiplexing gain translates into increased capacity for the system. A TDMA system can also take advantage of this large silence content in speech signals. So, the big debate in the US was about which system would offer a larger overall capacity for the available frequency bandwidth. Qualcomm, which first commercialized spread spectrum systems, claimed through various analyses that CDMA systems offered much higher capacity than TDMA systems. In the opposing camp, Ericsson and some other companies consistently rejected Qualcomm's claim. The main difficulty was that TDMA and CDMA systems are complicated, and it is difficult to settle the capacity question in a decisive manner. This discussion raged in the US for a few years, leading to the introduction of the TDMA-based IS-54 and CDMA-based IS-95 [3GW17, 3GW5] standards in the US in 1992 and 1993, respectively. IS-136, a revised version of IS-54 with a digital control channel specification, was published in 1994 [3GW4], followed by IS-136A in 1996 [3GW18]. These second-generation systems were introduced in the US later than the GSM system's introduction in Europe. In addition, the US market was fragmented into three parts, these two second-generation digital systems and the analog, first-generation AMPS system. In a sense, the situation in the US for second-generation systems is like what Europeans experienced at the time of first-generation systems: a multitude of systems and the resultant interoperability problems. This worked to GSM's advantage and remarkable success with 140 million GSM users worldwide now. IS-136 and IS-95 have about 93 million and 12 million users, respectively.

Yet another family of second-generation wireless systems is that of Personal Communication Networks (PCNs) or Personal Communication Services (PCS). The objective of PCS or PCNs is to provide ubiquitous wireless communications coverage, enabling users to access telephone networks for different types of communication needs, without regard for the location of the user or the location of the information being accessed [3GW11]. It is clear that this definition has much overlap with that for mobile phones. In fact, according to [3GW10], PCS presently means different things to different people! In the US, the FCC issued PCS licenses in the 900 MHz band for “narrowband services” and near 1900 MHz band for “wideband services” in 1995, 1996, and 1997 without placing any restrictions on the air interface and system architecture to be used or nature of services to be offered. PCS license holders began offering services in 1995. The industry, which not surprisingly includes the largest cellular companies in the US, and the standards organizations, has adopted seven technical approaches to wideband PCS. Suffice it to say that the distinctions between cellular systems and PCS will most likely disappear as third-generation wireless systems are developed and deployed.

The need for wireless data communication services has been recognized for many years. Today there is 4% data and 96% voice traffic in wireless systems. The volume for data traffic, however, is expected to rise sharply due to the use of the Internet and the worldwide web. By 2005, some industry sources predict that there will be 70% data and only 30% voice traffic. Furthermore, the number of wireless phone users has been sharply increasing over the past few years and this trend is expected to continue for at least the next decade. Some industry sources expect that there will be more wireless phones in the world than wired phones by 2003. The number of wireless users is expected to hit 800 million by 2003. These drivers have made it more important than ever to use the precious available frequency band as efficiently as possible. From a capacity point of view, it is now generally accepted that the CDMA system is more efficient than the TDMA system, although the gap between the two is not nearly as wide as Qualcomm had originally claimed. While flexibility and ease of engineering may partly explain the higher relative use of TDMA systems, CDMA systems are becoming increasingly refined. Progress has also been made in the development of other signal processing techniques and concepts for use in tomorrow's wireless systems. These include smart antennas and diversity techniques, better receivers, and hand over and power control algorithms with higher performance. Therefore, the search for third-generation wireless systems began a few years ago under the guise of Future Public Land Mobile Telecommunication System (FPLMTS) [3GW6] by the International Telecommunications Union. The name was later changed to International Mobile Telecommunication System 2000 (IMT-2000) in 1995 [3GW19, 3GW20]. The European efforts in this area started as the RACE (Research and Development of Advanced Communication Technologies) research program for development of the Universal Mobile Telecommunication System-(UMTS) [3GW19, 3GW20, 3GW7].

II.C 3rd Generation Wireless Systems

The IMT-2000 standard for third-generation wireless systems is presently under development by the ITU-R Task Group 8/1 (R stands for radio). The ITU plans to complete this task by the end of 1999, hence the name IMT-2000 standard [3GW21, 3GW8].

The IMT-2000 standard will offer users transmission rates up to 2 Mbits/sec, global roaming and interoperability, and a much wider array of wireless services. These should be contrasted with the second-generation wireless systems, which provide mainly voice service, some limited data communication capability (e.g., e-mail), and lack of interoperability due to the use of different systems and standards around the world. The transmission rate for second-generation systems is on the order of only tens of kilobits per second. Third-generation systems have the potential to offer users high data rate services such as web browsing (usually involving web pages with multimedia content) and even applications such as video teleconferencing. In the interim, and until systems based on the IMT-2000 standard are deployed some time between 2002 and 2006, the GSM operators plan to offer an enhanced version of the GSM system, called the EDGE system, with service rates up to 384 Kbps. EDGE employs a more spectrally efficient modulation scheme than GSM, as well as some other advanced techniques, but it is not as radical a departure from GSM as are the proposed third-generation systems. Some call EDGE a 2.5-generation system.

The deadline for submission of proposals for the air interface of the IMT-2000 system to the ITU was June 30, 1998. By that date fifteen RTT (Radio Transmission Technologies) proposals had been submitted, ten on terrestrial systems and five on satellite systems. A sixth satellite system, the Iridium system, was submitted to ITU after the expiration of the June 30 deadline. The Iridium proposal was accepted by ITU, and this brought the total number of RTT proposals under consideration to sixteen. These proposals were developed by national and regional standardization bodies and industry consortia in a handful of countries around the world. Between June 30 and September 30, 1998, these sixteen proposals were evaluated by ten evaluation bodies around the world. Not all evaluation groups evaluated all the sixteen proposals. As a matter of fact, all the evaluations and comparisons were based on the self-evaluations of the proposals made by the proposers themselves. No evaluation body had the time or resources to implement and simulate the different systems and carry out a more in-depth and unbiased evaluation of the proposals. The period between September 30, 1998 and March 31, 1999 has been designated by the ITU as the time during which harmonization of different proposals is to take place, and a single set of key characteristics for the IMT-2000 standard is to emerge. The following nine months until the end of this millennium have been reserved for further developing and refining the IMT-2000 standard until it is fully developed. During the year 2000, some field testing of the IMT-2000 standard is supposed to take place. Japan has the most ambitious goal of fully deploying an IMT-2000 system in 2001. Europe and the US are not expected to deploy such systems until about 2005. In the remainder of this section, we present an overview of the terrestrial and satellite RTT proposals, go over various inhibitors to success, and describe and motivate NIST work plans and strategy as far as the IMT-2000 and future standards for wireless communication systems are concerned.

II.C.1 IMT-2000 Terrestrial Proposals. Ten RTT (radio transmission technology) terrestrial proposals were submitted to ITU, four from the US, two from Europe, two from Korea, and one each from Japan and China. Only the following four RTT proposals are the major contenders for the IMT-2000 standard: the cdma2000 and the UWC-136 RTT proposals from the US, the W-CDMA (or UMTS Terrestrial Radio Access (UTRA)) from Europe, and the W-CDMA RTT proposal from Japan. The UWC-136 RTT proposal, which is an extension of the IS-136 standard, is the only TDMA-based proposal among the four. The other three are all based on wide-band CDMA. In fact, the UTRA and the W-CDMA proposals are so similar that with most likelihood they will merge into a single proposal, a very strong force for the US proposals to contend with. Therefore, the term W-CDMA will be used to denote this joint effort underway by the 3G Partnership Program (3GPP) Consortium. In the interest of brevity, the other six RTT proposals submitted to the ITU will not be discussed, except to mention in passing that the remaining two RTT proposals from the US have merged into a single RTT proposal called the Wideband Packet CDMA (WP-CDMA) system, which is much closer to the W-CDMA system than to the cdma2000 system.

All these cellular systems use 5MHz channels within each cell. The channel bandwidth is strongly (but not entirely) dependent on a parameter called the chip rate in a direct-sequence CDMA (DS-CDMA) system. A major difference between the cdma2000 and the W-CDMA systems is that the former uses a chip rate of 3.6864MHz and the latter uses a chip rate of 4.096MHz. The chip rate chosen for cdma2000 is three times that used in the IS-95 system, and this was done for the purpose of backward compatibility with IS-95. In case of W-CDMA, the chip rate was chosen so that it would be backward compatible with GSM and the system in use in Japan. Of course, there are many other differences between the two systems, but perhaps none as divisive as the choice of chip rate. All three systems, and all other systems proposed to ITU for that matter, offer users a variety of transmission rates up to 2Mbits/sec. In fact, all sixteen RTT proposals (including the six satellite RTT proposals) meet all the ITU requirements for the IMT-2000 standard. Whether a single standard will emerge from the ITU standardization effort depends on a number of factors, some of which are not technical. For example, the chip rate difference is due to the strong desire of the cellular system operators (service providers) to protect their investment in second-generation systems. Each operator would like to ensure that the IMT-2000 standard is, to the maximum extent possible, backward compatible with its second-generation system. Of course, it is not possible to keep everybody happy, because, together with the desire for having a system capable of offering worldwide roaming, that would mean expensive base stations and mobile user handsets as well as possibly an inefficient use of the frequency spectrum. This, and some other obstacles in way of having a single IMT-2000 standard for the whole world, is addressed later in this section.

IIC.2 IMT-2000 Satellite Proposals. A key difference between a terrestrial wireless system and a satellite wireless system [3GW22] is that it is simpler to provide global coverage with the latter. So, global roaming is a major selling point for the satellite systems. The drawbacks are the price of the service, the delay in communicating back and forth with a satellite in the earth orbit, and perhaps the reduced overall system capacity. It is very expensive to launch satellites to put base stations in the orbit. The satellite phones are also substantially more expensive than their terrestrial counterparts. The price difference depends on how high the satellite is in the orbit. The round trip delay of communicating with the satellite can lower the quality of service in real-time applications such as voice conversations and video teleconferencing. The reduction in capacity is due to the fact that a down-link satellite beam will cover a large geographic area on the earth. That makes frequency reuse difficult. Therefore, despite the huge investment of a number of companies in developing and deploying satellite systems for commercial cellular phone users, it is not expected that such systems would have nearly as large a market penetration as the terrestrial systems. It is sufficient to mention that users are expected to be charged anywhere from $3 to $6 per minute for phone calls made on a satellite mobile phone, and this is about ten times more expensive than the rate on terrestrial cellular systems. Therefore, mobile satellite phones will be attractive to users needing telecommunication capability and network connectivity in remote areas of the world or places that do not even have wireline phone service. This means that the market will require a class of customers for which price is not an issue or will require penetration into developing countries that do not have phone service. The percentage of the population in such countries that can afford using a satellite mobile phone and the extent of usage remains to be seen.

There is no strong reason that the six satellite RTT proposals should harmonize and merge into a single standard. Since they offer global coverage, it is perfectly OK for them to coexist as long as they can share the available frequency band. Given the high price of launching satellites and maintaining these systems, this is going to be a field for a small number of large players. From a business point of view, it may turn out that only one or two systems survive. For the satellite system operators, the ITU standardization process is like a seal of approval that may increase their chances of grabbing a larger share of the market. This seal of approval is not as crucial for them as it is for terrestrial wireless system operators.

II.D The Future of the Technology

Wireless telephony systems are here to stay in a big way, unlike some other wireless technologies, which are on the drawing board and may never turn into viable commercial products and services. Investment in the wireless telephony industry is at $50.1 billion in capital investments and $20 billion in spectrum auction fees in the US. There are more than 60 million wireless subscribers in the US now, and the average monthly bill per user was at just below $40 in 1998. It is anticipated that there will be 170 million wireless users in the US by 2007; that's more than 50% of the population.

The purpose of this subsection is to help identify a NIST role in this important area of information technology. Since the NIST role will be mainly in the terrestrial 3G systems, and it is an accepted fact that the ITU process will result in at least two standards (one for terrestrial and one for satellite systems), we concentrate on terrestrial 3G systems in the rest of this section. At the time of writing of this report, and within eleven months of the completion of the IMT-2000 standard, it is not clear at all whether a single, global standard for terrestrial wireless communication systems will emerge at the end of the ITU standardization effort. There are three major obstacles that have to be removed before there can be such a standard. The 16th Meeting of ITU-R TG8/1 in Brazil in March 1999 will determine how likely it is that these obstacles will be removed, and a single international terrestrial standard for 3G wireless systems developed by the end of 1999. Each of the major obstacles is discussed below.

II.D.1 Manufacturers' Interest. An IPR (Intellectual Property Rights) conflict between Qualcomm and the European Telecommunications Standards Institute (ETSI) has been in the news for the past several months. Qualcomm is the major force behind

TIA's cdma2000 proposal, and ETSI is the sponsor of the W-CDMA proposal backed by all the European countries. They are both based on wideband CDMA technology, where Ericsson and Qualcomm each have a number of patents. Although the best technical solution would need both sets of patents, it appears that the two camps are trying to find ways around each other's IPR. This would not result in the best technical solution. In summary, each manufacturer's interest is to influence the development of the IMT-2000 standard so that it is based on as much IPR from that manufacturer as possible. Naturally, this leads to a conflict of interest.

II.D.2 Operators' Interest. Each major operator providing cellular service has invested hundreds of million dollars in its present network and infrastructure. Each would like to see an IMT-2000 standard that is backward compatible to the second-generation (2G) technology they presently use. By backward compatible, we mean a system where an operator can use its existing network infrastructure as much as possible and where 2G and 3G systems can co-exist in a dual-mode handset (mobile terminal). One can have a dual-mode phone that would support GSM and UTRA (this is what GSM operators, ETSI and the European countries wish to have), a dual-mode phone that would support IS-95 and cdma2000 (this is what IS-95 operators and Qualcomm wish to have), or a dual-phone that would support 2G TDMA technology (such as IS-136) and UWC-136 (this is what an operator like Bell South likes to see happen). If a single standard is adopted, then many operators would have to spend a lot of money to change their systems, and this may just be too much for many of them to bear. Dual-mode phones are needed, because there will be a transition period where systems based on both 2G and 3G technologies will be operational. Of course, one can also think of multi-mode phones supporting more than two systems, but that would even further increase the price of the phones.

II.D.3 Spectrum Availability. One important promise of IMT-2000 is global roaming, and this requires availability of a single, sizable frequency band in all countries around the world. This is a major challenge, because spectrum allocations in different countries are different, and it is difficult to free up some frequency band that has already been allocated for other usage. For example, in the US, the FCC has auctioned some parts of the frequency spectrum. It is not possible to force the license holders to make their part of the spectrum available for IMT-2000 systems. The only remaining options are two. Would the license holders be willing to voluntarily use the spectrum for IMT-2000 systems? Would the license holders be willing to sell their licenses to service providers that wish to offer IMT-2000 services?

II.E Opportunities for NIST

The first question that comes to mind is whether there *is* a role for NIST. The answer to this question appears to be a resounding "*yes*". While the Federal Government insists that the industry and the marketplace should determine which technologies should be developed; it is important for the federal government to play an active role in the development of standards for certain areas of information technology, where existence of such standards would result in market growth and ultimately a boost to the US economy. Such standards would prevent or at least reduce interoperability problems. The economies of scale in equipment manufacturing that would result from strong standards would reduce the equipment cost for the users and operators alike and would make it possible for the US to better compete with other countries in overseas markets.

In the case of wireless communications, a technically strong and adequately staffed and coordinated program among key Federal Government agencies could have resolved the TDMA-CDMA wars of the early 1990’s in the US in a better way, possibly leading to improved industry dynamics. Had there been such a program, government scientists could have carefully evaluated TDMA and CDMA systems through analytical and overall system simulation means and then made the results of such a study available to the whole industry. There is a major difference between a particular company having large financial stakes in this market carrying out such a study and having a neutral, unbiased authority doing such. Companies would try their best to make their own technology look good, and the competitor's technologies look inadequate and inferior. Hence, company-generated evaluations would not carry as much credibility as the report from an accepted independent authority. The role of academia in evaluating such competing technologies should not be ignored. Universities play a very important role in developing new theories and inventing new techniques; however, they tend to stay away from evaluating in sufficient detail very complicated systems such as cellular communication systems. Academics simply do not have the resources for such a study. Even if the resources were made available to them, they may not be interested in such studies, because the work is not really the type of fundamental research work that doctoral students would need to get their doctorates.

NIST is the ideal agency in the US government for launching a technical program in wireless communications. The NIST mission of testing, measurements, and developing standards is exactly the type of work needed for evaluating various wireless technologies and for facilitating the development of industry-consensus national and international standards. Fortunately, such a program at NIST started at the beginning of Fiscal Year 1998, when the Information Technology Laboratory formed a Wireless Communications Technologies Group (WCTG). In its first year of operation, the WCTG was staffed with a handful of accomplished engineers with strong background and qualifications in basic and applied research. This is indeed a very good start, but the group really needs to grow if it is to make a significant contribution to the US industry and to the emerging standards in wireless communications. It should be noted that the WCTG work on wireless networks is only one of the three main areas the group is actively working on. The fact that the Group needs to expand is something that can be easily and independently verified.

Finally, it is important to explain more specifically how NIST WCTG plans to contribute to the process of developing the IMT-2000 standard and, more generally, to future wireless communication systems. The WCTG plan centers on developing a testbed for the W-CDMA and cdma2000 systems, and even possibly the UWC-136 system. This process has already started, and once these software simulation environments are in place, scientists in the group can evaluate the performance of specific systems under various channel conditions and traffic demands. For example, they can determine how well each system would perform if a user decides to do some web browsing via his wireless link while traveling on a train or in a car. What kind of voice and video quality one would get from the system? How does the system perform as a function of the number of active users? And, many other interesting questions like these can be investigated. Once the testbed is in place, the group will be able to study in depth individual components in wireless systems and make its own novel contributions to development of advanced signal processing and communications techniques and to protocols for wireless systems. In addition, the WCTG is already participating in the IMT-2000 standardization process and providing some technical input into the process.

The technical work and innovations in mobile phones will certainly not end with the development of the IMT-2000 standard. Since the technology is far from being mature, and there is plenty of room for improvements and for developing systems with higher performance, there will be a need for a standard for fourth-generation wireless communications in a decade or so. NIST has to start now and expand its programs if it is going to fill the present need for an unbiased, neutral evaluator of the wireless technology and play the major role we believe it should play at that time. There are many technical innovations that have not been fully exploited in the systems presently under consideration by the ITU. A few examples are turbo codes, smart antennas, beam forming, pencil beams, diversity techniques (space, time, frequency), multi-user detection techniques, and advanced compression and transmission techniques for multimedia information. It is also abundantly clear that there will be other novel techniques and methodologies developed in the next decade. NIST should play a major role in evaluating these technologies, facilitating their adoption in future standards, and even developing some of these ideas.

III. Broadband Wireless Systems

The market for broadband communications is growing rapidly, and the potential applications and services are numerous and diverse. Several technologies are currently being developed to offer such services. Both wired and wireless system solutions aim to win a share of the market. The wired contenders include digital subscriber lines (xDSL), cable modems and others. The wireless contenders include satellite communications systems, stratospheric communications systems, and terrestrial communications systems, specifically, Multipoint Multichannel Distribution Service (MMDS) and Local Multipoint Distribution Service (LMDS). While these systems do not all target identical market segments, the likely markets do overlap. The various broadband wireless access systems compete therefore more against high-speed wired solutions than against each other. Table III-1 from Allied Business Intelligence, Inc. presents a forecast of market share for various high-speed communication solutions [BWS1]. This forecast projects that wired technologies would command about 75 % of subscribers in the year 2003.

Table III-1. Broadband Subscribers by Technology, US Market, 2003
(source Allied Business Intelligence, Inc.)

ADSL	36 %
Cable Modem	26 %
ISDN	12 %
Satellite	12 %
LMDS	9 %
Others	5 %

III.A Terrestrial Broadband Wireless Systems

A common way to classify broadband terrestrial, wireless fixed communications systems is to call systems using frequencies below 10 GHz MMDS systems and to call systems using frequencies above 10 GHz LMDS systems. The motivation for this classification is that the propagation characteristics are quite different at say 30 GHz than at 5 GHz. Equipment and components for frequencies under 10 GHz are mature, while equipment at higher frequencies is based on technology that still is relatively new and expensive. Systems at frequencies above 20 GHz are for fixed users. Systems below 10 GHz are also for fixed users, but may evolve to serve mobile users.

III.A.1 MMDS (Multipoint Multichannel Distribution Service)

MMDS is often referred to as wireless cable [BWS2]. In 1996, the FCC auctioned off licenses in the 2150-2162 MHz band and the 2500-2686 MHz band in 493 markets within the US. In September 1998 the FCC cleared the way for using the spectrum for two-way digital services [BWS3]. New rules also allow more freedom for various other uses within these bands. This new authorization will effectively enable voice, video, and data over wireless cable. However, the bandwidth allocated to the return link is modest (2686-2689.6 MHz). A number of operators are offering commercially high-speed Internet access, where the telephone line is used as return link. Many trials are underway for wireless two-way data, voice and video communication.

III.A.1.1 Technical Overview. MMDS operators broadcast multiple TV channels or related services from an antenna located on a tower, tall building or mountain. The signals are received by microwave dishes typically about 40-50 cm in diameter, or perhaps larger in outlying areas. Information can be distributed within 25 or 30 km within line-of–sight from each main tower. A block down converter integrated into or mounted on an antenna mast translates the received signals into the band utilized by standard cable TV. A set-top converter identical in function to a standard cable TV channel selector is located near the TV receiver. Digital TV requires a set-top box for every television set. When Internet access is provided, the downstream data rate for individual subscribers can be up to 750 kbps.

The total data rate offered by a base station is on the order of 1 Gbps, depending on coding, modulation and roll-off factor. Sectorization will however increase this number. For instance, with a reuse factor of 18 (10 degree sectors), the cumulative downstream data rate for one base station is almost 20 Gbps [BWS4]. For upstream, the available bandwidth is much smaller, and a less complex modulation scheme is likely to be used to allow low power transmitters at the subscriber location. The data rate will therefore be much smaller, on the order of 6 Mbps, without sectorization [BWS5].

III.A.1.2 Prediction for the Future of MMDS. Some hard times have plagued the MMDS industry in recent years. For instance, in October 1998 Heartland Wireless Inc, America’s largest MMDS provider with approximately 165,000 subscribers, was de-listed from the NASDAQ stock exchange. Heartland reportedly failed to meet minimum closing bid and net tangible asset requirements. Residential users constitute the main market for MMDS systems, even though MMDS is being offered to small and medium businesses. The main applications for MMDS include TV, either broadcasting or on demand, and Internet access. The competition from cable companies and telephony companies is hard, leading some people to question the market viability of MMDS technology. MMDS systems have however the advantage that they run at a relatively low frequency. The cost of microwave components at 5 GHz is relatively modest, permitting low-cost customer premise equipment (CPE) and components that are readily available today. Introducting cellularization and sectorization into MMDS will however add complexity and cost to the system. Another advantage of MMDS systems is easy deployment. An MMDS system can be deployed typically in from two to six months.

Later this year some operators are planning to offer business Internet services over MMDS that compete directly with asymmetric digital subscriber line (ADSL) services [BWA20]. For example, DataChron, which offers MMDS in Boston and New York, charges corporate customers $99/month for access by one workstation and $249/month for access by ten or more workstations. DataChron also offers home service for $49/month. MMDS coverage for wireless digital TV is also expanding somewhat, especially in the territory covered by BellSouth.

III.A.2 LMDS (Local Multipoint Distribution Services)

As with MMDS, LMDS is a point-to-multipoint (PMP) solution that aims to overcome the “last mile” problem. In the US, LMDS systems utilize spectrum in the 28-31 GHz range. The total bandwidth is 1,150 MHz (block A) plus 150 Mbps (block B). Other bands are also allocated to LMDS-type of systems at 24 GHz and 39 GHz. In Europe the band from 40.5-42.5 GHz is generally used, but there are some differences between countries. For instance, in Germany the 24 GHz band is allocated to PMP services, while some other countries are using the 28 GHz band. Korea and Japan use frequencies from 22 GHz to 28 GHz.

III.A.2.1 Technical Overview. The cell size for LMDS systems varies from 3 to 8 km in radius. LMDS subscriber antennas are highly directional (beam width of 2 to 7 degrees) and flat plate, for mounting on window, roof, or wall. Several slave cells may be connected to a master cell using repeaters. In order to limit interference between cells, a number of interference suppression techniques can be employed, e.g., spatial separation, sidelobe rejection, polarization and frequency interleaving. Typically sectorization is used to enhance the capacity; here sector antennas provide service over a 90, 45, 30, 22.5 or 15-degree beam width.

The LMDS network structure consists primarily of 4 parts: network operation center (NOC), fiber-based infrastructure, base station and CPE. The NOC contains the network management equipment. The fiber-based infrastructure typically includes SONET OC-12, OC-3 and DS-3 links, central office (CO) equipment, ATM or IP switching systems and interconnections with the Internet and public switched telephone networks (PSTN). The base station equipment contains a network interface for fiber termination, baseband digital signal processing, up/down conversion and RF front-end (Rx/Tx) equipment. The CPE includes an outdoor unit (ODU) and an indoor unit (IDU). The ODU consists of microwave equipment, while the IDU provides digital processing for modulation, demodulation, control and CPE functionality.

Various network architectures, such as TV broadcasting and point-to-point (PP) and PMP data communication, are possible within an LMDS system design. Therefore both ATM and IP transport methodologies are practical.

III.A.2.2 Main Technology Players. There are several parties playing important roles in the development of LMDS technology. Large manufacturers, such as Ericsson, Lucent, Nortel, Raytheon and Alcatel, offer complete system solutions today, or will in the near future. Obviously, these suppliers will have a big impact on the development of LMDS as they promote their own solutions. Then there are sub-system manufacturers, which offer for instance Ka-band components. Then there are the LMDS operators. In February and March 1998, 104 American companies bought licenses at the FCC LMDS auctions. The capability of LMDS operators to compete with wired operators depends to a large extent on the development of low-cost system solutions. Finally there are regulatory and standardization bodies. The FCC's current policy cedes decisions on spectrum use to the LMDS operators and equipment suppliers; therefore, industry-led standardization bodies must play an important role by developing good standards that are widely accepted and used by the LMDS industry.

III.A.2.3 Standardization Bodies. Several national and international standardization bodies work on standards applicable to LMDS-type systems. The Digital Audio-Video Interoperability Consortium (DAVIC) and the European Telecommunications Standards Institute (ETSI) have released specific LMDS standards [BWS7-BWS8]. DAVIC is a Geneva-based, non-profit association with 204 members from 25 countries. The DAVIC 1.3 specifications have been available since June 1997, and include three wireless technologies: satellite communications, MMDS and LMDS. The DAVIC specifications provide interfaces for both narrowband and broadband core networks. Two frame structures are provided, one for MPEG-2 Transport Streams and the other for ATM-cell transfer. The ETSI LMDS specifications are based on the digital video broadcasting (DVB) specifications developed for 11/12 GHz satellite broadcasting. The purpose of the ETSI LMDS specifications is merely to provide interoperability with the DVB environment.

Specifications that are closely connected to LMDS are under development by the ETSI BRAN (Broadband Radio Access Networks) project [BWS9]. These specifications for private and business radio networks are known under the generic name of HIPERLANs (High Performance Radio Local Area Networks). The project is currently developing standards for three types of Broadband Radio Access Networks: HIPERLAN/2, HIPERACCES and HIPERLINK. The HIPERACCESS standard is the one having most relevance to LMDS-type systems. This long range (5 km) variant is intended for PMP, high speed access (25 Mbps) by residential and small business users to a wide variety of networks including the Universal Mobile Telecommunications System (UMTS) core networks [BWS10], ATM networks and IP based networks. Completion of the stable draft Functional Specifications is expected in the first quarter of 2000. The objective is to obtain low cost technology within 2002.

N-WEST (National Wireless Electronic Systems Testbed) [BWS1] is a project recently initiated by two agencies of the United States Department of Commerce: the National Institute of Standards and Technology (NIST) and the National Telecommunications and Information Administration (NTIA). N-WEST aims to promote the standardization of broadband wireless access systems, and in particular LMDS, through the IEEE 802 LAN/MAN Standards Committee. Different parties of the broadband wireless access industry, such as service providers, system integrators and component manufacturers, are invited to participate. The time schedule for the standardization work was to be established in January 1999.

III.A.2.4 The LMDS Situation in Europe. The European ACTS (Advanced Communications Technologies and Services) program [BWS11] includes a number of projects related to LMDS. CRABS (Cellular Radio Access For Broadband Services) is [BSW12] one of these projects where partners from seven European nations are collaborating to design a microwave cellular radio service using the 40.5 to 42.5 GHz band. Trials in five areas of Europe involve detailed studies of the system architecture necessary for implementation and for development of standards.

III.A.2.5 The Future of the LMDS Industry. Until recently, the main market for LMDS was considered to be residential users in areas where cable is impractical or too costly. The services provided would then be mainly TV, either broadcasting or on-demand, and access to the Internet. The standards developed by ETSI and DAVIC reflect this view. This situation however is changing. Ka-band technology is still quite new and components expensive. The cost of CPE will be at least $1000, too expensive for single homes. Industry projections estimate that the cost must come down to maybe $200 for the home market to take off. The winners of the FCC LMDS auction also seem very reluctant to launch services for residential users. The biggest license holder, WNP Communications, has stated an intention to first offer LMDS services to big companies, where a large number of users will share each LMDS link. The communication services will then be close to PP, and the conception of the system is very different from a system providing a mix of TV broadcasting and low-rate bursty data communication to a large number of users. Later WMP Communications will offer service to medium size companies. Residential users will not be offered LMDS services before the year 2005, at the earliest. By that time, the market for high-speed access for home subscribers will probably be safely in the hands of wired providers, offering xDSL services or cable-modem services.

One LMDS Internet service provider, CellularVision, operates commercially in New York city, serving parts of Manhattan, Brooklyn, and Queens [BWS21]. Cellular Vision charges only $200 for installation of required access hardware, and then charges $80/month for unlimited access. Download speeds for individual subscribers range around 1.5 Mbps; however, since CellularVision has implemented LMDS as a downstream service only, the upstream channel must be provide by some other medium, typically a telephone line. This offering indicates that LMDS providers could perhaps compete with providers of xDSL and cable-modem services.

III.B Stratospheric Communication Systems

Stratospheric or high-altitude communication systems provide an approach somewhat in between terrestrial LMDS/MMDS and satellite communication systems. At least four companies in the US are now developing stratospheric telecommunications networks using high-altitude planes or balloons to serve as sort of tall antennas or very low satellites, depending on the perspective. In the US, these systems will need to file with the FAA for flight permission as well as with the FCC for transmission frequencies.

III.B.1 HALO. HALO stands for High Altitude Long Operation. The platforms are manned aircraft with pilots working in shifts. Piloted aircraft are used to avoid regulatory and technological problems. Angel Technologies Corporation [BWS13] is currently busy promoting its system to attract potential partners.

The HALO aircraft will maintain station at an altitude of 52 to 60 thousand feet by flying in a circle with a diameter of about 5 to 8 nautical miles. Three successive shifts on station for 8 hours each can provide continuous coverage of an area for 24 hours per day, 7 days per week. The “Cone of Commerce” footprint will be from 50 to 75 miles in diameter, and can be divided in up to 15 beams. For instance, in Los Angeles, 10 million people could be served within a footprint. Using this approach, about 100 sites would serve 72 % of the US population.

Angel Technologies hopes to lease frequency spectrum in the 28 GHz band or the 38 GHz band, and to resell LMDS-like CPE to carriers and corporate customers. In order to do this, they plan to partner with traditional LMDS companies. Frequency reuse with a factor of 1:5, 1:7 or 1:9 will be used to optimize the utilization of the frequency resources. Plans include laser communication with Low-earth orbiting (LEO) satellite systems.

The first HALO aircraft made its maiden flight on July 26, 1998. Plans call for a first operational system during the year 2000, with Los Angeles selected as the first market. Angel Technologies estimates that a 1.5 Mbps connection would cost about $40 a month.

Solutions using manned aircraft have the advantage that regulations already exist. The HALO aircraft have already received permission from the FAA to fly. Currently, no regulations cover balloons, and according to Angel Technologies, balloons could face years of regulatory hurdles. The HALO system may therefore win the competition with the balloons, even though plane-based systems should prove more complex to design and deploy and more expensive to operate.

III.B.2 Sky Station. The Sky Station System [BWS14] plans a network of geostationary platforms deployed in the stratosphere for up to ten or more years. These platforms will be balloons or aerostats of variable size, depending on market demand. Normally, a Sky Station platform will be approximately 157 meters long and 62 meters in diameter at the widest point. The capacity of a platform is 2 Gbps dynamically spread across the footprint, equivalent to 425,000 8 kbps telephone calls with 50 % voice activity [BWS15]. Equipped with a Sky Station user terminal, subscribers will be offered broadband services ranging between 2-10 Mbps. The plan is to launch at least 250 Sky Stations positioned at about 22 kilometers altitude over areas of greatest population. Additional Sky Stations may be added at any time.

According to Sky Station Systems, Stratospheric Telecommunications Service (STS) will commence with the first Sky Station deployment in 2001. After that, additional Sky Stations will be launched one per week until all populous parts of the world are covered by STS. Each Sky Station provides STS to an area of approximately 19,000 square kilometers or 7,500 square miles. Sky Stations will be implemented in accordance with subscriber demand as expressed by responsible organizations in each country.

The Sky Station System will operate in the 47 GHz frequency band (47.2-47.5 GHz stratosphere-to-Earth and 47.9-48.2 GHz Earth-to-stratosphere). The FCC will auction this band (47.2-48.2 GHz), where potential users will include stratospheric platforms and satellites. Harmful interference is anticipated with the Radio Astronomy

Service, which has a primary allocation in the 48.94-49.04 GHz band. Radio astronomy is extremely vulnerable for interference downward from the sky.

III.C Satellite Communication Systems

A large number of broadband satellite systems have been filed. Some of them have a rather speculative nature, and only a few have a chance to be built. Two different approaches can be distinguished, the geo-synchronous earth orbiting (GEO) approach using a small number of geostationary satellites, and the low earth-orbiting (LEO) or medium earth-orbiting (MEO) approach using larger constellations of non-geostationary satellites. These LEO and MEO systems are sometimes referred to collectively as non-GEO systems (NGEO). Other potential orbital configurations are high earth-orbiting (HEO) constellations and hybrid constellations. Most of these systems will use the Ka-band, which is virtually unused and contains much more room than the lower L-, C- and Ku-bands traditionally used for satellite transmissions. The Ka-band satellites use a number of new technologies, such as on-board processing and switching, inter-satellite links (ISLs) and multiple pencil-like spot beams. These satellites allow "bandwidth-on-demand", which will considerably reduce the costs for most subscribers. In addition, ISLs will eliminate the need to bounce signals back and forth from ground to space repeatedly to move signals around the globe.

Ka-band satellite communications have experienced a sudden interest since the middle of this decade, and the commercial risks, at least for GEO systems, are considered less than for LEO/MEO mobile satellite systems (MSS) such as Iridium, Globalstar and ICO [BWS16]. Although the potential of Ka-band satellite systems is promising, there are many challenging technical issues that require further studies. The research and development establishment continues to work on developing onboard processing (OBP) equipment to meet the bandwidth, power, and mass requirements for these satellites. New techniques to improve the transmission performance are needed in order to reduce the size and cost of earth stations. In addition, inter-linking solutions must be provided between these satellite networks and other wireless and wired networks.

III.C.1 Non-GEO Systems. The two main non-GEO competitors are Teledesic [BWS17] and SkyBridge [BWS18]. After dropping its Celestri system, Motorola has become involved in Teledesic, both financially and probably as a main contractor for the satellite payloads. Matra Marconi Space is also involved in Teledesic, probably dropping its own system WEST. Teledesic planned an initial service offering in 2003, but lately it has been stated that service will not be available before 2005. The constellation size is not yet fixed, apparently it will consist of about 100 satellites.

SkyBridge is a 64 satellite Ku-band system. Unlike Teledesic, which will basically provide backbone transmission, SkyBridge will provide communications directly to end subscribers. As a response to the alliance between Motorola and Teledesic, SkyBridge is now marketed alongside Cyberstar via a partnership with Loral. This consolidation will stack the combined offerings of Globalstar, Cyberstar, and SkyBridge against the combined offerings of Iridium, Celestri, and Teledesic. SkyBridge will begin offering its service by the end of 2001.

III.C.2 GEO Systems. Since GEO systems comprise satellites that are fixed relative to the earth, many problems, such as the hand over of earth station coverage and the complex management of inter-satellite links can be avoided, and the equipment complexity is reduced because phased-array antennas are unnecessary. GEO systems may not be a good solution for interactive multimedia communication, though, thanks to the increased propagation delay incurred when bouncing signals to and from satellites positioned approximately 22,500 miles above the earth.

The GEO systems considered most likely to be built and deployed include Spaceway from Hughes, Astrolink from Lockheed-Martin and Cyberstar from Loral. Hughes has extended Spaceway to include 20 NGEO satellites. Both Spaceway and Astrolink will start service in 2001. Cyberstar is already up and running with a limited service, called StarService, which offers one-way communication using a Ku-transponder in Loral Skynet's Telestar 5 satellite. This service will be enhanced to include two-way communication, and CyberStar will later launch its own Ka-band satellites.

III.C.3 The Future of the Technology. Broadband service is the last of three distinct groups of new satellite-based services to get off the ground, following behind voice services and paging services. Satellite systems offering broadband services are generally complex to design and build and expensive to deploy. The initial investment is on the order of billions of dollars. Even though Iridium can be viewed a technological success, being the first operational LEO system to offer voice services, the question of its financial viability remains open. Satellite systems offering broadband services face large technical and economic risks. At present, forecasts regarding the future for this technology remain uncertain.

III.D Opportunities for NIST

Projections for broadband wireless access systems foresee a large potential market, which will undoubtedly begin its growth over the next 5-10 years. The competition with wired technologies is however intense. Consideration of opportunities for NIST must be divided into three technological categories: satellite systems, stratospheric systems, and terrestrial systems.

Satellite systems are affected by the highest risks because huge initial investments are necessary, and long lead times are needed to move a system from design to operation. Only the largest companies in the business have the possibility to launch such systems. These companies, or alliances between these companies, have the experience and competence to develop the technology, or they carefully select their sub-contractors to provide the necessary expertise. The substantial investment and high risk involved in such systems suggest that the main players will not be receptive to contributions that NIST can make. NIST should therefore stay out of this business.

The future for stratospheric communication systems remains somewhat hazy. These systems are relatively new in the commercial arena. Essential subjects such as frequency bands and flight permissions are not yet clear. Only a few stratospheric communication systems projects can be identified, and none of them have yet the financial base they need to become operational. Given the early days, uncertainty of a viable market, and the uncertainty of the economic impact if such a market develops, NIST should stay out of this business as well.

The situation for terrestrial broadband access systems is quite confusing. System suppliers see their system solution implemented in every network in the country, sub-system and component manufacturers see their product in every system solution, while the operators are doing market research to find out which services the market wants.

There is little collaboration among the various players. To have a chance to win market share from wired technologies, this situation needs to change. One approach is to develop standards that the industry can agree upon, and then comply to. This is a difficult task because of conflicts of interest within the industry. In this situation NIST might play an important role.

IV. Pico-cell Wireless Systems

Pico-cell wireless technologies deliver radio coverage and connectivity to devices within a short-range, on the order of 10 to 100 meters. Up until now, such short-range communication has been of interest in radio controlled toys in the Part 15, unlicensed band. In the 1980s, pico-cells became of interest for delivering indoor radio services, particularly for cordless phones (CT-2 and DECT). Recently, pico-cells are gaining further interest to provide wireless data and multimedia to untethered end terminals, and as replacement for cables to provide connectivity among personal computers, phones, sensors, and other accessories. Dominant and emerging pico-cellular technologies for this new application include the wireless local-area network (LAN) defined by the IEEE 802.11 standard and two wireless multi-device communications specifications, one being defined by the Bluetooth consortium and one being defined by the HomeRF consortium. As these pico-cell technologies mature, they will fill an important void in the development of wireless networking by providing mobile users with easy access to the Internet, and by providing new technologies for sensor networks and for device-to-device communication in localized areas. These technologies can launch an important new market that will encompass component, device, and service providers, as well as software developers.

IV.A Indoor Cordless Telephone Systems

The cordless telephone standards, CT-2 [PCW1] and DECT (Digital European Cordless Telephone) [PCW2], emerged as pico-cell cordless standards for residential use. These served primarily to provide more than one phone line for home and business subscribers. Both standards included a few basic data capabilities, DECT more so than the CT-2. DECT, a time division multiplexing (TDM) technology with the capability to assign channels automatically and dynamically, continues to be used to a fair degree in Europe, as a cordless phone standard. DECT was, and continues to be, a prime candidate for many small-cell outdoor environments, and for connecting pico-cells with larger cells based on TDM, specifically cells deployed with GSM-compliant cellular telephony services [PCW3].

IV.B Wireless Local-Area Networks

Wireless local-area networks, or LANs, cover two general technological approaches, one using infrared signals and the other using radio frequency signals. Both technologies have been incorporated into the physical layer of the approved IEEE 802.11 wireless LAN, discussed below. In addition, some other approaches to infrared wireless LAN technology are being pursued within the Infrared Data Association (IrDA). Both the IEEE 802.11 wireless LAN standard and the work of IrDA are discussed in turn below.

IV.B.1 IEEEE 802.11 Wireless LANs. Following a prolonged standards-setting process, the IEEE recently adopted the 802.11 wireless LAN standard [PCW4, PCW10].

The standard, originally intended for small office cable-less automation connecting personal computers and workstation with peripherals, is also suitable for ad-hoc networking in conferences and meetings. The 802.11 standard uses a slow frequency hopping radio frequency (RF) or infra-red (IR) shared, spread-spectrum link standard of 1 and 10 Mbps. Carrier-sense multiple access (CDMA) and reservations are used in combination to support both data and voice traffic on the same network. The system can either operate in a centralized mode (with assigned base stations) or a decentralized mode (with peer-to-peer interactions). The physical layer supports radio frequency transmission, as well as infrared transmission. The 802.11 standard for wireless LAN is not compatible with either the Bluetooth specification [PCW5] or the HomeRF specification [PCW6], which are discussed below in section IV.C. First, the work of IrDA is considered.

IV.B.2 Infrared Data Association (IrDA). The technology and protocols for infrared data transmission (IrDA DATA) and control signals (IrDA CONTROL), being developed by the Infrared Data Association (IrDA), fall somewhere between wireless LANs and wire replacement networks, intending to support both applications [PCW13-PCw15]. In general, IrDA DATA is recommended for high-speed (up to 4 Mbps) short range, line of sight, and point-to-point data transfer. The IrDA CONTROL standard is recommended for same-room connection of cordless peripheral to a PC.

IrDA DATA specifications call for transmission ranges between contact and 1 meter; however, the publications report that typically 2 meter ranges can be achieved. Experience shows that alignment between transmitter and receiver can be critical in order to achieve high data rates. A low-power implementation of the standard limits transmission range to 20-30 cm. While a maximum data rate of 4 Mbps is specified, some implementations may provide as little as 9,600 bps bi-directional communication, with step increases in performance up to 115 Kpbs units specified by the standard. Other implementations can provide a synchronous serial infrared transmission link at 1.152 Mbps. The top speed link definition achieves 4 Mpbs. Two different cyclic redundancy codes (CRCs) are defined depending on the speed rating of the implementation: CRC-16 for 1.152 Mbps and CRC-32 for 4 Mpbs. The IrDA standards define a number of link-layer (e.g., IrLAP and IrLMP), transport-layer (e.g., Tiny TP and LM-IAS), and application-layer protocols (e.g., IrTran-P, IrOBEX, IrLAN, IrCOMM, and IrMC) designed for wireless transmission environments.

For control devices, IrDA CONTROL achieves bi-directional communication at up to 75 Kbps over a range of up to 5 meters. Each IrDA CONTROL port enables a PC to communicate simultaneously with up to eight peripherals.

IV.C Wire Replacement Networks

Electronic devices that employ short-range radio links have found their way into the daily lives of many people within the past decade. Widespread applications include cordless phones, keyless entry for automobiles, garage door openers, and file transfer in portable computers. Current uses however, are in general restricted to single devices (two transceivers) or a group of very similar devices (e.g., laptop computers). Two recently initiated industry projects, Bluetooth and HomeRF, promise to broaden the use of wireless connections by specifying standard links for a wide range of electronic devices. While both efforts intend to enable wireless communications and interoperability between devices, each is geared for a different type of user. Bluetooth is aimed at the mobile user, while HomeRF is centered on the personal computer for users in the home. In addition to replacing cables, these technologies provide a means for networking groups of devices and for establishing connections with wired data networks.

IV.C.1 Bluetooth. Bluetooth, a consortium established in 1998, claims to offer a robust and low cost technology to business and mobile users who need to establish a link or a small network to connect their computer, phone, and other peripherals and accessories [PCW11, PCW12]. The technology creates a common air interface to all devices that can be connected, and aims to create, among other things, services around the cellular phone. This technology is being promoted by Ericsson and Nokia, who are two of the main competitors in the cellular telephony business (competitors coming together to create new markets), along with IBM, Intel, and Toshiba. More than three hundred companies have signed licensing agreements to adopt the Bluetooth technology. Bluetooth technology can provide connectivity among the cellular phone, laptop, personal digital assistant, headphones, mouse, and other accessories. In addition, the technology can also provide for end user interoperable cellular connections (e.g., CDMA and TDMA) via a small router, with a back-end Bluetooth interface for all end devices, and multiple front-end cellular interfaces.

Bluetooth radios utilize the publicly available 2.4 GHz ISM frequency band for transmission. Operation in this band does not incur usage fees and permits global use of Bluetooth devices. The main technical difficulty associated with operating in the 2.4 GHz band is the effects of interference from nearby devices. To combat these effects, Bluetooth employs frequency hopping at 1600 hops/second, forward error correction, and retransmission. Bluetooth will support full-duplex voice and data transmission, including simultaneous voice and data channels. The maximum gross data rate is currently 1 Mb/s, with plans for an increase to 2 Mb/s in second generation systems.

Embedding Bluetooth radio modules in portable battery operated devices will be possible due to the small size, low power consumption, and low cost of the modules. Two variants of the radio module are scheduled for production: a short range and a medium range module. The short-range version, built into a 9x9-millimeter microchip, will support links of up to 10 meters and will consume 1 mW of power. The longer range module will include a power amplifier to extend the range to a maximum of 100 meters. Up to 8 Bluetooth devices may network by sharing the total bandwidth, with one of the devices coordinating the transmissions once connections are established. A standby mode is used to facilitate additional devices without dividing the bandwidth further.

The Bluetooth specification encompasses both the physical and the data link layers, along with a cryptographic scheme for provisioning security. Table IV-1 gives a summary of the current specifications for Bluetooth. More details may be found at the Bluetooth web site [PCW5].

IV.C.2 HomeRF. The Home RF consortium aims to provide secure wireless private network connectivity among all home electronic devices including phones, PCs, laptops, palmtops, television sets, and other addressable electronic devices, which potentially include alarms, cameras and recording equipment. The HomeRF Working Group, formed in March of 1998, consists of over 70 companies including IBM, Intel, Microsoft and Motorola. Successful deployment of HomeRF technology will enable many home services including traditional intercom, access to the Internet from a variety of terminals, and management of security alarms and other home control devices. The HomeRF market is expected to develop around the personal computer in the home. Devices, in addition to being directly linked via the HomeRF interface, could also connect via this radio interface to a Universal Serial Bus (USB). The HomeRF specification, though adopting a frequency hopped shared spread-spectrum link, is distinctly different from the Bluetooth specification and from the wireless LAN specification.

Table IV-1. Planned Specifications for Bluetooth Version 1.0

- Range 10 Meters in shirt pocket or briefcase
- Network Size: 8 devices per pico-net
- Max. Gross Data Rate: 1 Mbps
- Frequency: 2.4 GHz and 1600 Hops/sec
- Supports 3 near line-quality voice links
- Optimized for cell phones and mobile devices
- Multi-point to point connections
- Point-to-point TCI/IP support
- Low power standby mode
- Higher transmit power possible
- Based on a working prototype
- More: http://www.bluetooth.com
- Main players: Ericsson, IBM, Intel, Nokia, and Toshiba

The HomeRF specification, dubbed Shared Wireless Access Protocol (SWAP), is based on existing cordless phone (DECT) and wireless LAN (IEEE 802.11) technology. As in Bluetooth, transmission occurs in the 2.4 GHz ISM band, and frequency hopping is employed for frequency spreading; however, the hopping rate for HomeRF is a lower 50 hops/second. As is the case for Bluetooth, HomeRF supports full duplex voice and data transmission. An additional "ConnectionPoint" is required to coordinate a HomeRF system for time-critical applications, such as voice. Time-division multiple access (TDMA) is employed for these time-critical services, while CSMA with collision avoidance (CSMA/CA) is the multiple access method for packet data. A single HomeRF network may accommodate up to 127 devices, with a maximum raw data rate of 2 Mb/s. HomeRF modules will have a range of 50 meters without line of sight restrictions and will consume 100 mW of power. Table IV-2 gives a summary of the current specifications for HomeRF. More details may be found at the HomeRF web site. [PCW6]

IV.C.3 The Future of the Technology. With the high level of industry support for Bluetooth and HomeRF, these technologies are sure to find their way into many consumer devices in the near future. The first Bluetooth products are scheduled to be available in late 1999. Digital cameras, cordless headsets, mobile phones, portable computers, slide projectors are all likely candidates for Bluetooth technology. With the completion of the SWAP 1.0 specification in January of 1999, HomeRF is also well on its way to product releases by the end of 1999. Thirteen companies have already committed to build products based on HomeRF technology. Applications for both technologies will include wireless Internet access, networking of home computers and computer peripherals, connecting cordless phones enhanced for interaction with personal computers, and connecting remote display pads to nearby computers.

Table IV-2. Planned Specifications for HomeRF Version 1.0

- Range: 50 Meters in home and yard
- Network Size: unlimited
- Graoss Data Rate: 1 Mbps or 2 Mbps
- Frequency: 2.4 GHz and 50 Hops/sec
- Supports 6 near line-quality voice links
- Optimized for home voice and data
- Peer-to-peer networking
- Native TCI/IP support
- Low power paging mode
- Lower transmit power possible
- Based on shipping 802.11 and DECT technology
- More: http://www.homerf.org
- Main players: AMD, Ericsson, HP, IBM, Intel, Microsoft, Motorola, National Semiconductor, and more

IV.D Opportunities for NIST

While NIST should monitor all developments in the pico-cell technology area, immediate, active involvement in a subset of these technologies is critical. Specific opportunities, including on-going activities involving the NIST Information Technology Laboratory, are discussed below.

IV.D.1 Protocol and Interface Specifications and Product Interoperability. Two of the pico-cell technologies, Bluetooth and HomeRF, are currently undergoing development through their respective consortia. Both consortia will be releasing the first version of the specifications in 1999. Further refinement of these specifications is expected in subsequent releases. The refinement of specifications, as well as interoperability testing, is expected to go well into the year 2000. In each of these cases, NIST, through its expertise in modeling, specification, and testing of networking protocols and interfaces, can assist the consortia to develop test suites and to identify potential ambiguities, inconsistencies, and errors in the specifications, and to suggest improvements in the specifications. Additionally, several vendors will be developing products using the specifications, and many others, including computer and telecommunications equipment vendors, will be integrating the specifications into their products. Thus, interoperability will be a critical issue for the success of these products. NIST can work with industry to develop interoperability tests and procedures, and can serve as a neutral party to organize interoperability testing.

As of fall 1998, the Advanced Networking Technology Division (ANTD) is a member of the Bluetooth Consortium. The initial contributions of the ANTD to this forum will be in the form of specification modeling. Later, we expect to assist in interoperability. At present, ANTD has no formal involvement with the HomeRF consortium, but is considering contributing to this forum as well.

IV.D.2 Multi-mode Pico-cell Devices. As pico-cell devices proliferate, interoperability across different pico-cell environments will become a serious issue for users. For example, users will desire a personal digital assistant (PDA) or a laptop computer to operate seamlessly in their car (Bluetooth), at home (HomeRF), and say, at a conference (wireless LAN). Lack of such interoperability will dampen the growth of these markets. Since these environments have totally incompatible interfaces, the device either would have to be equipped with all the interfaces, which will be costly and technically complex, or else some other cost-effective solution will have to be found. A potential solution is based on building an adaptable device, which will automatically configure itself, via either software or via FPGA (field-programmable gate array) design, to the appropriate interface after the device detects a change in its environment. Such an adaptive solution, which permits the device to configure itself to one of many modes (with accompanied adjustments in power, coding/modulation, and signaling), might still be a useful solution to explore, although some of the efficiency made possible by integrated design of the individual interfaces may be lost. Facilitating interoperability across environments by exploring multi-mode designs, and thus cross-fertilizing the markets, is potentially an area where NIST can contribute to the development of pico-cell technologies.

IV.D.3 Lightweight Protocol Suite (UPLANET). Protocols that reliably transfer data over pico-cell links must be lightweight and must efficiently utilize the limited RF bandwidth, as with any other wireless technology. Currently, the UPLANET (Unwired Planet) consortium [PCW7] is developing such protocols, and their primary target is data transfer over current emerging cellular and personal communication system (PCS) technologies [PCW8]. The protocols range from data link to higher layer protocols such as web access, multi-media, ad hoc networking, file transfer, and encryption.

These issues are relevant for pico-cell environments as well, and the solutions developed for cellular environments may need to be customized. These issues can be expected to also arise in Bluetooth and HomeRF arenas, after their respective interface specifications are complete. In particular, the higher layer issues arise because each consortium has its own specified lower level pico-net architecture, media access, and radio resource management.

A significant area of protocol development in which the ANTD is involved is mobile ad-hoc networking, which considers how devices with a pico-cell RF interface come together and form an ad-hoc network. Forming an ad-hoc network involves discovering devices, establishing a topology, and controlling data transmission among a set of mobile devices. At present, there are eight proposals at the Internet Engineering Task Force (IETF) as candidates for a standard Mobile Ad-hoc NETwork (MANET) protocol. ANTD, in collaboration with DARPA, is working through IETF to conduct an unbiased performance evaluation of these proposals, as well as to communicate the military requirements for MANET protocols. This evaluative work on MANET protocols could steer the course of future protocol development for pico-cell networks. MANET is discussed further in a subsequent section on future wireless technologies.

IV.D.4 Performance Evaluation for Product Evolution. While the wireless LAN and the DECT/CT-2 specifications are complete, and the specifications and initial design of both Bluetooth and HomeRF will soon be complete, the performance evaluation of these products leading to the next stage of product evolution is just beginning. To understand what can be expected, consider, for example, the several vendors (IBM for one) now working on wireless LAN products, which comply with the IEEE 802. 11 specification, but which have data rates in the range of 20 to 40 Mbps, significantly higher than the rate specified in the original standard. These increased rates can be achieved through improved coding and modulation techniques. These improved techniques, while offering higher data rates, can co-exist with the older, standard interfaces. Similarly, performance evaluation of Bluetooth and HomeRF technology is likely to lead to new techniques that will be the basis for a next generation of a backward-compatible, higher-performance line of products. The ANTD is evaluating the performance of Bluetooth and is conducting research on and techniques for obtaining high performance in Bluetooth products. The issues under investigation include coding and modulation, multiple access, resource allocation, and protocol design. Similar activity for HomeRF is also being considered by ANTD.

IV.D.5 Integration into Systems. Devices equipped with pico-cell interfaces such as Bluetooth, HomeRF, or Wireless LAN, will likely be embedded in sensors and in systems with many potential applications, including electronic aides in meetings and conferences, bedside systems in hospitals, automobile entertainment and information systems, military sensor networks, and a host of similar applications. Successful development of such systems will require a design methodology for building reliable and secure network services based on distributed computing over fairly low bit-rate pico-cell links. Especially crucial will be the eventual role of mobile code in such systems. More will be said about mobile code in the next section. The ANTD has initiated a project, ***AirJava***, to advance the state-of-the-art in the design of systems based on mobile code and pico-cell wireless technologies [PCW9].

V. Software for Mobile and Embedded Devices

The expansion of wireless telephony over the past decade has caused a concomitant growth in the market for portable telephone handsets. This simultaneous growth of wireless telephony and portable phones should continue with the advent of third generation wireless telephony. More significantly, this record of joint growth between wireless telephony and portable phones foreshadows an even larger growth in both portable and embedded devices as wireless communications capabilities expand to include pico-cellular wireless technology. The future will find a wide range of small, portable and embedded devices outfitted with pico-cellular wireless transceivers. Such devices include personal digital assistants, notebook and laptop computers, digital cameras, audio-visual equipment, sensors and actuators, automobile entertainment and information systems, cellular telephones, computer peripherals, digital notepads, large-screen interactive displays, and wearable components, including glasses, pens, wristwatches, wallets, and radio-frequency tags. This huge expansion in the market for portable and embedded wireless devices suggests that opportunities will arise to create and market software development environments and tools specialized for small devices. Movement can already be seen in this direction. This section considers two specific software elements where NIST might find opportunities to assist the information technology industry. The first element is operating systems for portable and embedded devices. The second element is discovery and access services, that is, software for finding and accessing devices, services, and information within useful distance of a specific location.

V.A Operating Systems

Prompted by emerging markets for sophisticated cellular telephones, for personal digital assistants, for set-top boxes, and for automobile entertainment and information systems, a number of software companies have recently been investing considerable resources into development of operating systems for small computers [OS1]. The market battle for these operating systems appears interesting because portable and embedded devices tend to use a wide range of new processors designed for low-power consumption and heat dissipation, while also providing reasonable processing speed. In effect, these devices are not yet captive of Intel chips; thus, the market for operating systems remains open. While all of the current operating systems can be considered proprietary at this stage, three different classes of operating systems can be discerned. The first class includes real-time operating systems that are likely to remain proprietary. While many such operating systems exist, this report examines only two: GEOS [OS2, OS3] and PalmOS [OS4, OS5]. The second class includes proprietary operating systems that have pretense to become a de facto standard. At present, this class includes only the Microsoft Windows CE operating system [OS6-OS8], which this report examines. The third class includes proprietary operating systems based on a virtual-machine architecture. The best current example, examined in this report, is JavaOS [OS9-OS13]. After discussing these four operating systems, the report considers opportunities for NIST.

V.A.1 Propriety Operating Systems. Since the best current examples of handheld portable devices encompass the cellular telephone and the personal digital assistant, the report considers one operating system used to program each of these devices. The first operating system, GEOS 3.0, provides the programming environment for the state-of-the-art Nokia 9000. The second operating system, PalmOS, provides the programming environment of the PalmPilot, which established a new market for personal digital assistants (PDAs).

V.A.1.1 GEOS 3.0. The GEOS operating system, developed by Geoworks, a small software company located in Alameda, California, requires about 500 Kbytes of memory to execute. The operating system is intended for use in programming smart cellular telephones, pagers, and PDAs. Since the software is not tied to any particular hardware company, Geoworks markets the system across the world, particularly targeting the Japanese market, where many small, portable and embedded devices are designed and manufactured. Probably the most well known system to use GEOS is the Nokia 9000 cellular telephone. Another notable GEOS user is the Toshiba Genio PDA. While GEOS runs on small devices, most of the software develop occurs on a larger platform, such as a Windows NT machine. Most of the software that runs on GEOS is written in C++. The GEOS software development kit (SDK) includes an emulator so that GEOS applications can be tested in the Windows environment before downloading to a small device. In addition, the GEOS SDK contains various utility programs to convert data, such as bit maps, from Windows form to GEOS form. The GEOS SDK also includes a graphical user interface library that programs can use to interact with the user. To provide networking, GEOS includes a socket library under which protocol implementations for specific communications media can be inserted. In effect, GEOS leverages the Windows operating system as a development environment, but provides a proprietary operating system environment on which developers can implement software for small, wireless devices.

V.A.1.2 PalmOS. The PalmOS was developed specifically to provide an execution environment for the PalmPilot PDA. Since the PalmPilot consists of a Motorola "Dragonball" microprocessor (low-power version of the 68000), a serial port, and a limited amount (32 Kbytes) of execution memory (so-called random-access memory, or RAM) and non-volatile program memory (so-called read-only memory, or ROM), the PalmOS was designed specifically for this restricted environment. The PalmOS is also used in the Qualcomm pdQ product, which is based on the Motorola 68000.

The basic PalmOS consists of a run-time environment for the PalmPilot, along with some built-in applications; the environment and applications are held in ROM on the device. Integral to the PalmOS in ROM is the concept of synchronization between the volatile memory in the PalmPilot and a mirror copy held on a personal computer. In effect, the PalmPilot includes software, which runs on a personal computer, to provide a user with access to his PDA data through a desktop computer. The software on the desktop and the PalmOS can synchronize their copies of the data in volatile memory. This data can include both personal information and PalmPilot programs. In this manner, the PalmPilot can be extended to add programs, at the cost of space for storing personal information, up to the limits of the memory in the PalmPilot (typically 1, 2, or 4 M bytes).

To develop applications for the PalmPilot a programmer uses standard development tools on a personal computer, typically a Macintosh computer using a Motorola 68000 processor; however, any development environment should suffice provided that it can generate code for the Motorola 68000. Program code is written in C, C++, or assembler. The PalmOS development environment includes a PalmPilot simulator. The programmer can link his code with the simulator and then test it on the personal computer. When a program is ready, the programmer simply places it into a specific directory and synchronizes the personal computer with the PalmPilot. At that time, any new applications are loaded into the PDA.

V.A.2 Possible De Facto Standard - Windows CE. Based on the success of the PalmPilot, Microsoft has worked to stimulate a market in competing PDAs that will all run an operating system, Windows CE, developed by Microsoft. In addition, to the PDA market, Microsoft is working hard to establish Windows CE in the set-top box market and in the automobile entertainment and information market. In effect, Microsoft hopes to establish Windows CE as a de facto standard execution environment for portable and embedded devices. This will be a significant challenge for two reasons. First, the processors available in these markets are quite varied, and so Microsoft will have a lot of code porting to perform. Second, folks in these industries are cautioned by Microsoft's success at dominating the personal computing market.

Windows CE has the largest memory footprint (2 Mbytes) of any operating system competing for a share of the small device market. In addition, Windows CE is the slowest among these operating systems. Despite these facts, Windows CE has the broadest support among producers of handheld devices and applications. One reason for such support is that Windows CE includes a large number of applications, programming features, and supporting software for hardware components. A second reason might also be the solid network of business relations developed by Microsoft as it took control of the operating system market for personal computers. Will Windows CE become an appropriate operating system for the handheld digital wireless devices? This remains an open question because Windows CE is not particularly efficient in its use of memory and processing cycles, nor does it provide significantly advanced features for managing low-power devices.

Windows CE, designed independently from any other Windows operating system, is a multitasking, multithreaded operating system designed for 32-bit processors, but independent from any specific chip. The operating system has been ported to at least three chips: MIPS R4000, Hitachi SH3, and, of course, Intel x86. The full operating system requires 4 Mbytes of ROM and 2 Mbytes of RAM in order to execute. While this might seem like a lot of memory, the operating system includes a host of application software, such as Internet software, an e-mail client, a version of Internet Explorer, a graphical user interface similar to Windows 95, some personal information management software, and software to synchronize between applications in a handheld and the full versions of similar Microsoft applications that run on a personal computer. Based on the Windows CE software, Microsoft has developed hardware specifications for a handheld device to compete with the PalmPilot. Several companies now offer PDAs based on the Microsoft specifications.

Windows CE provides the software developer with an application-programming interface (API) that is compatible with the de facto standard Win32S API offered on Microsoft's other operating systems. The Windows CE API appears to be a subset of the full Win32S API, offering 500 functions instead of a 1000 or more. In addition, Windows CE has to add some functions that have no natural equivalent in the Win32S API. As with other operating systems for small devices, Windows CE applications are developed on a larger machine, running the Windows CE SDK on a standard Windows system. Software is typically written in C++. The development environment contains a Windows CE emulator that runs under Windows NT on Intel x86-compatible chips. The developer creates a x86 binary to test his application on the emulator. To create the application for another chip, the program must use a compiler capable of generating code for multiple chips. Once the compiler has generated appropriate code, the new application can be loaded to the portable device using the Windows CE synchronization mechanisms, much like the PalmOS.

V.A.3 Virtual Machine-based JavaOS. Sun Microsystems introduced, developed and marketed Java, a new approach to programming that is especially well suited for network-based applications. Java allows programmers to write a program once, and then to run that program on any type of computer in a network without recompiling or altering the source code. This feat is accomplished by compiling Java source programs to a byte-code format that can be interpreted by implementations of the specification for a Java Virtual Machine (JVM). Provided that the JVM is implemented correctly on all target computers, any Java byte-code program can execute on any computer. Well things are not quite that simple because serious Java programs rely on a number of Java foundation classes that deliver graphical user interface services, networking services, and file services. This means the serious Java run-time environments must map these foundation classes to underlying functions provided by the host operating system. In addition, the Java language contains constructs, such as threads, which might be most efficiently implemented by mapping these language constructs to services in a host operating system. These facts, coupled with the market dominance of Microsoft's

Windows operating systems, have led to a market situation where Microsoft has been tinkering with the JVM and mappings for the Java foundation classes. While Sun has taken Microsoft to court over these issues, Sun has also been pursuing a technical response - JavaOS - that Sun hopes can unseat the market dominance of Windows. While this might appear unlikely in the marketplace for personal computers, JavaOS has a chance to overcome Windows CE in the battle for market share among portable and embedded devices.

JavaOS 1.0, released in March 1997 for the Sun Sparc, X86, and StrongArm RISC chips, consists of a JavaOS microkernel, a Java run-time, device drivers, graphical user interface (GUI) software, networking software, and software implementing the Java foundation classes. In addition, JavaOS can be augmented with some applications, notably the HotJava web browser. The JavaOS microkernel, implemented in a platform dependent manner in C and assembly language, provides elemental operating system services, including booting, exception handling, thread, timer, and memory management, monitor implementation, interrupt and direct-memory access handling routines, a file system, and debugging and platform control features. The Java run-time, implemented in a platform independent manner in C, provides the JVM and the garbage-collection algorithm. Every other function in JavaOS, including all device drivers, networking software, and GUI software, is implemented in Java. Using this approach, JavaOS provides a full Java programming environment on a computer platform without the need for a host operating system, such as, say, Windows.

To implement the entire JavaOS system, including the HotJava browser and 1 Mbytes of bitmaps for fonts, a device must provide 4 Mbytes of ROM (for the code) and 4 Mbytes of RAM (2.5 Mbytes for run-time state and 1.5 Mbytes for downloading code, images, and web pages). For applications that do not require GUI software or the HotJava browser, the JavaOS can run in half this amount of memory. In effect, JavaOS can be tailored to fit specific applications, such as PDAs and set-top boxes; however, Sun Microsystems most tune the JVM and the garbage collection algorithms to support at least soft real-time applications. In its smallest possible configuration, JavaOS requires 512 Kbytes of ROM and 128 Kbytes of RAM. Additional memory is required for applications.

Development of JavaOS applications can, of course, be carried out on Java systems hosted on any computer and then downloaded to a platform running JavaOS. In addition, Sun Microsystems is working with software tool vendors to deliver a rich software development environment aimed specifically for JavaOS applications. The envisioned environment will include a remote debugging capability. Sun and IBM have teamed to develop a version of JavaOS specifically tailored for network computers.

V.A.4 The Future of the Technology. The future of operating systems for portable and embedded devices is hard to call. For cell phones and PDAs, it seems likely that the conventional path of applying proprietary real-time operating systems will continue to prevail over the foreseeable future. The risk is low, the technology is well understood, and technical and marketing relationships have already been established. Still, Microsoft has a potential to disrupt this market with Windows CE. For network computers, set-top boxes, and automobile entertainment and information systems, Microsoft and Sun seem well positioned to battle it out with Windows CE against JavaOS. The real opportunity for Sun will arise in the market for pervasive computing, based on the need for ad hoc networking among groups of portable and embedded devices that come and go among islands of wireless communications that are also connected to the Internet. In these applications, the mobile code capability provided by Java, which can be equaled at present by no competitor, rises to the fore. Section V.B.1, just ahead, describes the Jini services being built atop Java, That discussion illustrates some of the possibilities.

V.A.5 Opportunities for NIST. NIST has little opportunity to help the industry building proprietary operating systems for portable and embedded devices. This includes the Windows CE crowd, where Microsoft will act as the standards-setting broker. Most of the opportunities for NIST lie in the developments related to Java. This includes JavaOS, Java remote-method invocation (RMI), and Jini services. This new technology holds a vast potential to revolutionize computing and networking. NIST should provide whatever support it can to push this revolution ahead. Such support can include technical work within the ITL, as well as funding support from the Advanced Technology Program (ATP) for distributed computing technology based on mobile code. Regarding the technical opportunities, ITL can work with the Java industry to develop system designs and demonstrations showing how Java, JavaOS, and Jini can be combined with pico-cellular wireless technology and Internet technology to provide a networking foundation for pervasive computing. ITL can measure the performance of Jini technology in such an environment and can suggest areas for improvement. ITL can also propose and evaluate various security mechanisms and systems that will be required to make pervasive computing real. ITL can also help the industry to agree on a protocol architecture that will enable Jini services to interoperate with the Internet services that pervade the wired networking world. In addition, ITL can help industry to investigate mechanisms for carrying multimedia data across wired and wireless networks and into portable devices.

V.B Discovery and Access Services

The emergence of wireless pico-cell technology will enable people to carry or wear small devices into spaces where those devices can communicate wirelessly with each other and with devices embedded or residing in the spaces, including gateways to the wired Internet. This opportunity calls for the development of protocols and software techniques that will enable devices to discover and access each other, as well as services provided locally in a space or remotely on the Internet. Two developments in this area are underway already. One development is Jini, a discovery and access service based on Java [DAS1]. The other development is the Service Location Protocol, a protocol to support a discovery and access service for the Internet [DAS2]. Each of these is discussed in turn.

V.B.1 Jini. Jini is a discovery and access service based on Java technology. The operational concept behind Jini works as follows. When a service-providing device is newly connected to a network, the device searches for a directory into which it can deposit a description of the services it provides, as well as Java byte codes that enable a client device to access the provided services. When a client device is newly connected to a network, the device searches for a directory of services and then searches that directory for specific services that the client wants to use. When an appropriate service is discovered, the client downloads the byte codes deposited by the service-providing device and uses the byte codes to invoke the service. This deceptively simple and powerful capability requires a complex programming and protocol infrastructure to actually work.

To enable Jini, Sun Microsystems extended the JVM to support event distribution among JVMs connected by a network. In addition, Java RMI was extended to enable the use of multicasting, which is required to search for Jini directories. On top of these extensions, Sun Microsystems developed interfaces, formats, and protocols for interacting with Jini directories. These specifications permit a great deal of flexibility in the interactions between Jini clients, services, and directories. For example, a client can deposit in the directory a standing order for a desired service that is not yet available. In this manner a client can be notified should such a service become available. Whenever a service or a request for service is added to a directory, the directory entry contains a lease, or lifetime. Beyond that time, the entry is no longer kept in the directory. In this way, as services and clients vary, old entries are purged from the directory. On the other hand, clients and services that are hanging around must keep their directory entries up to date. Jini also provides transaction services that applications can use to ensure that all required services in a set are available before proceeding. All of these low-level Jini interfaces, formats, and protocols have been combined to form JavaSpaces, a distributed persistence and object exchange mechanism for Java objects.

The real power underlying Jini comes from the use of Java byte codes to provide interfaces to remote services. For example, imagine a PDA running the JavaOS. Once the PDA discovers a JavaSpace, finds a service for a remote projector, and downloads the byte codes providing a GUI to control the projector, a user can then begin using his PDA to remotely control a projector that was unknown before entering the room. To really envision the power of this approach, imagine that the PDA, the Jini directory, and the projector were all connected wirelessly with Bluetooth technology.

V.B.2 Service Location Protocol. An IETF group is also working toward an Internet discovery and access protocol called the Service Location Protocol (SLP). The SLP envisions that computers connected to the Internet will run a user agent (UA) that applications can use to discover and access services on the Internet. In addition, SLP foresees that each service offered on the Internet will execute a service agent (SA). In its most general incarnation, SLP also envisions a directory agent (DA) that can manage lists of services available within some scope. SLP provides services and protocol mechanisms similar to Jini. The details differ of course. The main conceptual difference between the two approaches is the use of Java byte codes by Jini. While SLP does not preclude the use of Java byte codes, SLP does not depend upon it. For this reason, the access portion of the discovery and access service is largely omitted from the current SLP specification. Two issues addressed by SLP, yet omitted from the current Jini specifications, are scope and naming. The SLP permits services to be grouped by scope (administrative, geographic, or topological) and then to be assigned to a specific DA. For naming, the SLP adopts the uniform resource locator (URL) scheme devised for the worldwide web. This means that SLP names are location dependent. Rather than matching against templates that represent serialized byte codes (as Jini does), SLP use keyword-attribute pairs to describe the capabilities of services. SLP does not include the capability for clients to submit standing queries to DAs. For this reason, a UA must poll a DA to watch for the arrival of needed services that are not available at startup.

V.B.3 Future of the Technology. The work on service discovery and access protocols should grow in the future. While Jini and SLP represent good beginnings, the capabilities specified only scratch the surface of the future needs. Because these initiatives are only beginning, NIST has an opportunity to contribute to a new technology development in support of tomorrow's pervasive computing environments.

V.B.4 Opportunities for NIST. ITL can, of course, adopt our usual role of building early research prototypes to evaluate the soundness of the specifications and to provide other researchers with a platform to use when exploring issues surrounding service discovery and access. In addition, ITL can attempt to erect both Jini and SLP discovery and access services for the resources on the NIST campus. In fact, we might attempt to merge the Jini and SLP ideas into one service. Using such a trial service, ITL could provide technical contributions to the relevant industry groups. This might be a good cooperative project between the networking research and service groups within ITL.

VI. Security Issues for Wireless Information Technology

The difficulty of securing computers in networks, as well as computer networks themselves, has received significant political and economic attention over the past decade. Unfortunately, despite the technical attention that has also been given to these difficulties, many issues remain unsolved, some would say unsolvable. The same thorny security issues inhibit the safe use of wireless information technology. But in addition, wireless technology is vulnerable by its very nature because the transmission signals travel through the air, rather than through shielded conduits. This section of the paper reminds the reader about the security problems that plague computer networks in general, and gives special attention to the increased vulnerabilities and difficulties faced in a wireless communications environment. Two special topics are also addressed: mobility and multicast. First, since many small devices are likely to be carried around the "edge" of the wired network, the security needs and constraints for small, specialized, mobile devices must be considered. Similarly, since mobile code is likely to play an increasing role in both wired and wireless networks, the paper considers some of the threats and countermeasures relevant when programs move among computers in a network. Second, since multicast protocols provide the foundation for many of the discovery and access services that will be deployed in a few years, the paper also discusses the special problems that arise when attempting to provide secure communication among groups, whether across wired or wireless channels.

VI.A Wireless Communications Security

Due to its physical broadcast nature, wireless communications are generally more vulnerable to malicious and accidental threats than their wired counterparts. As a result of this inherent vulnerability, security is a mandatory component of wireless communications. While it is more difficult, and potentially more important to secure wireless communications, the issues, threats and the respective required services to adequately respond to these threats are mostly the same for wired and wireless technologies. On the other hand, the task of providing security services for wireless networks is more complicated than in the wired case. Power and bandwidth limitations, often non-existent in wired networks, impose considerable constraints on the complexity and efficiency of security protocols [WCS1]. Also, security services will have to operate across very long distances, where policies and services will have to be negotiated between home base stations, relays, and mobile units.

The remainder of this section will briefly highlight the security services required to protect wireless communications against particular threats, and then will discuss the components required to implement these services. In addition, the section identifies the unsolved issues surrounding these components. The final subsections discuss the future of wireless communication security, and suggest some opportunities for NIST.

VI.A.1 Threats and Services. There are many aspects of wireless communications that are vulnerable to accidental and malicious threats. A set of security services, confidentiality, integrity, availability, authentication, and non-repudiation, have been defined by the US Government [WCS2] to protect against these threats. The following is short discussion of these services. More information on these services can be found in [WCS3] and [WCS4].

Confidentiality services are primarily used to protect user and signaling data from passive eavesdropping attacks. They are also used, particularly in wireless environments, to prevent against traffic analysis. Traffic analysis detects when a user is connected to the network, and obtains the identity and location of the user. Integrity services ensure that modifications to data are detectable. These services protect against active attacks such as the insertion, deletion, and modification of data. They also protect against the replay of data. Availability services detect and combat denial of service attacks or attacks that degrade service. Such threats can be either accidental or malicious. Availability services also prioritize access and egress to wireless networks. Authentication services verify the identity of a claimed source of data. These services are used to verify mobile units to each other, mobile units to and from the network, and users to mobile units. Non-repudiation services are used to verify transactions through the use of a trusted, independent third party. These services provide accountability between mobile units and between mobile units and network managers.

VI.A.2 Services for Wireless Communications. Network security services are typically implemented as combinations of cryptographic algorithms, wrapping-unwrapping functions, challenge-response protocols, and key exchange protocols. The following provides a brief description of these components, and discusses specific issues regarding wireless communications.

Cryptographic algorithms provide the core protection for wireless communication. Cryptographic algorithms can be placed into three categories, encryption algorithms, one-way hash algorithms, and digital signature algorithms. Encryption algorithms provide confidentiality and integrity. One-way hash algorithms provide integrity, availability, and authentication. Digital signatures provide authentication, integrity, and non-repudiation. Because of their complexity and overhead, the strength of any particular algorithm must be weighed against its use in a wireless environment. Wireless communication devices are typically small, mobile units with little computational ability. Such devices can be easily overwhelmed by the computational demands of strong cryptographic algorithms.

Wrapping-Unwrapping functions take unprotected data to be transmitted across a wireless network and, through the application of cryptographic algorithms, encapsulate the data in a secure envelope, providing the required security services. Upon receipt of protected data, these mechanisms then verify that the packet is secure, remove the protective envelope, and pass the data to the appropriate application. These functions are fairly simple and easy to implement in a wireless system.

Challenge-response protocols provide authentication and access control services. Typically, the complexity of these protocols can be managed by providing varying levels of protection. Selected protection levels would be easy to implement within the constraints of wireless devices. These protocols often require fast authentication and encryption algorithms to verify the data and the identity of the remote entity as well as to prevent simple forms of denial of service.

Secure communications between two entities begins with some shared secret or key. Obtaining that key is often the most complex component of network security. In wireless communications, mobile units are typically hardwired with a master key. A copy of this key is kept at an authentication center and is used to authenticate the mobile unit and to generate session keys if additional security services (e.g., encryption) are required [WCS5]. This approach to key exchange does not scale well; thus, relies on the physical security and longevity of the master key. If the master key ever becomes compromised, all of the security services are compromised.

In some instances (e.g., CDPD networks) keys are generated upon request between mobile units and authentication centers using the Diffie-Hellmen key exchange protocol [WCS1, WCS3]. The generated key is then used to authenticate other devices, assuming the channel between the authentication center and the other devices is secure. The problem with this approach is that there is no authentication between the mobile unit and the authentication center. This makes it possible to attack the mobile unit by impersonating the authentication center. Additionally, some lightweight techniques are needed for integrated authentication and key exchange for data encryption because doing these tasks separately leads to vulnerability to "man-in-the-middle" attacks.

Wireless networks require a more robust key exchange mechanism similar to the one defined in RFC2408 [WCS6]. In addition to a stronger and more robust dynamic key exchange mechanism (similar to the second example above), RFC2408 includes an additional component, a public key certificate, which would allow the mobile unit to verify the authenticity of the authentication center. It should be possible to design a key exchange protocol equivalent to RFC2408 that works within the physical constraints of wireless communications. One issue that certainly needs technical consideration, however, is the design of lightweight security protocols (so-called micro or nano-cryptograhy) that can provide good security for short messages without using heavy-duty encryption techniques, which require large overhead. Lack of low-overhead cryptography has been widely perceived as one inhibitor to the growth of wireless data for financial transactions.

Most of the existing wireless services typically implement security mechanisms at the link layer, providing security on a link-by-link basis [WCS1, WCS5]. As network technology continues to grow, networks will become increasingly heterogeneous, requiring data to transit across trusted and untrusted, wired and wireless networks. For this reason, users will come to demand more robust end-to-end security services. Link-by-link services will have to be complimented or replaced by the addition of network and application security services.

The final component necessary for the complete integration and use of these security services is policy control and management. Users of wireless communications currently know very little about the underlying security services and have no control over them. As additional services are included and more robust security services are implemented, applications, network managers, and users will want the ability to specify their security policies for any particular transaction. The underlying infrastructure will have to translate this policy into security service requirements and then select automatically the appropriate options, protocols, and algorithms to implement the requirements. These transformations will be extremely complex; solutions are just now being discussed and developed for wired networks. The wireless community should participate in these discussions so their requirements can be addressed.

VI.A.3 The Future of the Technology. The future of wireless communication depends on scalable, robust, and efficient security technology. Most of the security technology being developed today is scalable and robust, but would operate poorly within the constraints of a wireless communication system. As a result, only minimal security services are provided for wireless communications, making wireless networks far more vulnerable than wired networks. To improve this situation, several steps must be taken. Security services across wireless networks must be implemented end-to-end. Authentication services and key exchange technology must become more robust, including a mix of secret key and public-private key management technologies. As more security services become implemented, and as these services become more complex, sufficient policy management must exist to inform users about the available services and to let users select those services required for any particular transaction.

VI.A.4. Opportunities for NIST. NIST, and particularly ITL, is in a unique position to work with the wireless community to define improved security technology for wireless communications. The security services required for wireless communications are similar to those required for wired communications. ITL has been recognized as a leader in defining and enabling network security technologies. By focusing on the constraints of wireless technology, ITL can assist in adapting existing security technology and in defining new security technology for wireless communications.

VI.B Mobility

Wireless communications leads directly to small, portable devices that can be carried by a person on the move. In addition, some of the discovery services proposed for wireless networking environments are based on mobile code. For these reasons, special consideration must be given to security issues relating to mobility of devices and code.

VI.B.1 Mobility of Devices. Mobile devices are subject to the same threats as non-mobile, or tethered, devices. Some of these threats, however, may pose a greater security risk to mobile devices than their tethered counterparts. For example, mobile devices are more susceptible to eavesdropping on, or interception of, their wireless communications. Eavesdroppers don't have to install sniffers on networks, deploy Trojan horses, tap into physical communication links, carefully position themselves to monitor the electromagnetic radiation of electronic devices, or risk being caught trespassing. Conventional encryption techniques offer proven countermeasures to the threat of eavesdropping. These techniques will be employed only when the contents of the communication need to be protected from eavesdropping and contain sensitive information. Peer mobile devices must be able to negotiate encryption protocols as each device may have different encryption/decryption capabilities. Encryption also carries a computational and communication cost that will affect the use of this countermeasure.

Jamming wireless signal transmissions is also unique to mobile devices. Although there haven't been many occurrences of this type of denial of service attack on existing mobile devices, as the use of these devices increases and the deployment of mobile networks becomes more prevalent, these risks must be carefully assessed and corresponding countermeasures developed. The intelligence and military communities have dealt with these signal-jamming issues for many years, but commercially viable solutions within the cost, size, and time-to-market constraints are not yet available. Entire mobile networks could be subject to this denial of service if countermeasures and fault-tolerant and fault-recovery techniques are not employed.

Physical security threats such as theft and hardware tampering also pose greater risks to mobile devices. Intricate schemes for stealing laptop computers at airport security checkpoints have been widely reported. Thieves have cloned cellular phones by intercepting and reusing identifying codes. These are examples of some of the new risks faced by mobile devices that stray out of the confines of a typical office environment. Physical security controls and mutual trust of other employees in an office environment may allow some employees not to worry much about requiring users to login to their desktop. A desktop computer is less likely to be lost or stolen than a laptop computer or other mobile device. Access control to mobile devices, however, must be strictly enforced as anyone in the possession of these devices can masquerade as its legitimate owner. Alternative authentication mechanisms, such as biometric techniques, will become necessary as the number of mobile devices increases, because users will find it increasingly difficult to remember passwords or to carry special hardware. Mutual authentication of peer devices will also be necessary as both the service requestor and service provider may masquerade as unauthorized users.

Administration of security policies for mobile devices will require additional study as the administrative domain of mobile devices may be continuously changing as users frequently join new ad hoc mobile networks. These solutions must be robust and scaleable as each user will have several networked mobile devices and can assume a different role within each network.

VI.B.2 Mobility of Code. Over the years computer systems have successfully evolved from centralized, monolithic computing devices supporting static applications, into client-server environments that allow complex forms of distributed computing. Throughout this evolution limited forms of code mobility have occurred: the earliest being remote job entry terminals used to submit programs to a central computer and the latest being Java applets downloaded from web servers into browsers. A new phase of evolution is now under way that goes one step further, allowing complete mobility of cooperating applications among supporting platforms to form a large-scale, loosely-coupled distributed system.

The catalyst for this evolutionary path is mobile code - programs capable of suspending their execution on one computer and moving to another computer where they resume their execution. A spectrum of differing shades of code mobility exists, corresponding to the possible variations of relocating code and state information, including the values of instance variables, the program counter, and the execution stack.

[MC1] A number of models exist for describing mobile code systems for comparative [MC1] or for standardization purposes [MC5-MC6]. However, for discussing security issues it is sufficient to use a very simple model, consisting of only two main components: the mobile code and the mobile code platform. In this simple model, the mobile code comprises both the code and the state information needed to carry out some computation. The mobile code tends to be static or unchanging, while its state information may vary dynamically, reflecting the results of the actions it has taken.

VI.B.2.1 Overview of Mobile Code Threats. Threats to security generally fall into four comprehensive classes: disclosure of information, denial of service, corruption of information, and interference or nuisance. There are a variety of ways to examine in greater detail these classes of threats as they apply to mobile code systems. Here, we use the components of the mobile code model to classify the threats, in order to identify the possible source and target of an attack. It is important to note that many of the threats that are discussed have counterparts in classical client-server systems and have always existed in some form in the past (e.g., executing any code from an unknown source either downloaded from a network or supplied on floppy disk). Mobile code simply offers a greater opportunity for abuse and misuse, broadening the scale of threats significantly.

Four threat categories can be identified: threats stemming from mobile code attacking a platform, a mobile code platform attacking mobile code, mobile code attacking other mobile code on the platform, and other entities attacking the mobile code system. The cases of mobile code attacking mobile code on another platform and of a platform attacking another platform are covered within the last category.

VI.B.2.1.a Mobile Code against Mobile Code Platform. Incoming mobile code has two main lines of attack. The first is to gain unauthorized access to information residing at the mobile code platform; the second is to use its authorized access in an unexpected and disruptive fashion. Unauthorized access may occur simply through a lack of adequate access control mechanisms at the platform or through masquerading as mobile code trusted by the platform. Once access is gained, information can be disclosed or information residing at the platform, including instruction codes, can be altered. Depending on the level of access, the mobile code may be able to completely shut down or terminate the mobile code platform. Even without gaining unauthorized access to resources, mobile code can deny platform services to other mobile code by exhausting computational resources, if resource constraints are not established or not set tightly.

VI.B.2.1.b Mobile Code Platform against Mobile Code. A receiving mobile code platform can easily isolate and capture mobile code and may attack it by extracting information, corrupting or modifying its code or state, denying requested services, or simply reinitializing or terminating it completely. Mobile code is very susceptible to the platform and may be corrupted merely by the platform responding falsely to requests for information or service, or delaying the mobile code until its task is no longer relevant. Extreme measures include the complete analysis and reverse engineering of the mobile code's design so that subtle changes can be introduced. Modification of the mobile code by the platform is a particularly insidious form of attack, since it can radically change the mobile code's behavior (e.g., turning trusted mobile code into malicious mobile code) or the accuracy of the computation (e.g., changing collected information to yield incorrect results).

VI.B.2.1.c Mobile Code against Other Mobile Code. Mobile code can target other mobile code using several general approaches. These include actions to falsify transactions, eavesdrop upon conversations, or interfere with the mobile code's activity. For example, attacking mobile code can respond falsely to direct requests it receives from a target or even deny that a legitimate transaction occurred. Mobile code can gain information by serving as an intermediary to the target mobile code (e.g., through masquerade) or by using platform services to eavesdrop on intra-platform messages. If the platform has weak or non-existent control mechanisms, then mobile code could even directly interfere with other mobile code by invoking its public methods (e.g., attempt buffer overflow or reset to an initial state), or by accessing and modifying its data or code.

VI.B.2.1d Other Entities against Both. Even assuming that the mobile code and platform are well behaved, other entities both outside and inside the mobile code framework may attempt actions to disrupt, harm, or subvert the mobile code framework. The obvious methods involve attacking the mobile code and inter-platform communications through masquerade, (e.g., through forgery or replay) or intercept. For example, at a level of protocol below the mobile code-to-code or platform-to-platform protocol, an entity may eavesdrop on messages in transit to and from mobile code or platforms to gain information. An attacking entity may also intercept mobile code or messages in transit and can modify their contents, substitute other contents, or simply replay the transmission dialogue at a later time in an attempt to disrupt the synchronization or integrity of the mobile code framework.

VI.B.2.2 Countermeasures. Many conventional security techniques used in contemporary distributed applications (e.g., client-server) also have utility as countermeasures within the mobile code paradigm. Moreover, there are a number of extensions to conventional techniques and techniques devised specially for controlling mobile code and executable content (e.g., Java applets) that are applicable to mobile code security. We review these countermeasures by considering those techniques that can be used to protect mobile code platforms, separately from those used to protect the mobile code that runs on them. Farmer, et al. [MC7] provides an alternate perspective by classifying, from easy to impossible, commonly sought security objectives and associated conventional techniques that can be applied.

VI.B.2.2.a Protecting a Mobile Code Platform. Without adequate defenses, a mobile code platform is vulnerable to attack from many sources, discussed earlier. Fortunately most conventional protection techniques, traditionally employed in trusted systems and communication security, can be used to provide analogous protection mechanisms for the platform. This is due in large part to the traditional role hardware plays as the foundation upon which software protection mechanisms are built. That is, within the mobile code paradigm, the platform is a counterpart to a trusted host within the traditional framework. Conventional security techniques include the following.

- Mechanisms to isolate processes from one another and from the control process.
- Mechanisms to control access to computational resources.
- Cryptographic methods to encipher information exchanges.
- Cryptographic methods to identify and authenticate users, mobile code, and platforms.
- Mechanisms to audit security relevant events occurring on the platform.

Similarly, more recently developed techniques aimed at mobile code and applicable to mobile code security have evolved along those same traditional lines. These include the following.

- Developing mobile code using an interpreted script or programming language.
- Limiting the capabilities of the languages so that they are considered "safe".
- Applying digital signatures to mobile code and other information to indicate authenticity.
- Restricting the mobile code's capabilities on a platform by constraining resources (e.g., lifetime, storage), by controlling service access (e.g., network destinations, directory segment), and by making capabilities location dependent.

The Java programming language and runtime environment [MC2] illustrate the nature of the recently developed techniques listed above. There are many mobile code systems based on Java, including Aglets [MC3], Mole [MC8], and Voyager [MC9]. The Java environment includes built-in security controls for isolating code into mutually exclusive execution domains and for verifying the byte codes downloaded from class files. The Java environment also inherently supports code mobility, dynamic class loading, digitally signed code, object serialization, platform heterogeneity, and other features that provide an ideal foundation for mobile code development. The Java security model for version 1.2 [MC13] contains a new permission-based mechanism for constraining the computational capabilities of mobile code, which also can benefit mobile code systems based on Java. Each permission specifies the authorized access to a particular resource, such as a connect permission to allow access to a given host and port. The Aglet security model [MC14], for example, to a large degree reflects Java's underlying protection mechanisms.

Other notable interpreted systems include Telescript [MC10] and Agent TCL [MC11]. The latter is based on Safe TCL [MC12], which employs a padded cell concept as a counterpart to Java sandboxes. The term padded cell denotes an isolation technique whereby a second interpreter pre-screens any harmful commands from being executed by the main interpreter. Similar mechanisms, to those in Java for constraining mobile code, have been built into Telescript, Agent TCL, and Telescript's successor, Odyssey [MC15].

VI.B.2.2.b Protecting Mobile Code. Because mobile code is completely a software entity, the traditional view that hardware protects software applies only when the set of platforms the mobile code visits can be trusted to some degree. Assuming the mobile code trusts its home platform to provide the required support services and not subvert its activities, countermeasures in the form of conventional security techniques can be applied on behalf of the mobile code via the platform. These measures rely primarily on identifying and authenticating trusted parties prior to interacting with them. The measures include the following.

- Issue users and platforms public key certificates for strong authentication.
- Convey information (e.g., mobile code and messages) securely (i.e., with confidentially, integrity, source authentication, and non-repudiation) among platforms.
- Detect and ignore replay attacks against platforms.
- Audit platform services and other security-related events for post processing analysis and detection.

VI.B.2.2.c Limits of Conventional Countermeasures. Conventional security controls generally work fine for static code, but eventually break down, as mobility becomes increasingly unrestricted. The basic dilemma is that mobile code needs to travel and work autonomously, but protecting mobile code from unknown mobile code platforms is very difficult to achieve. This vulnerability results in a double-edged problem. When mobile code hops between platforms, the receiving platform cannot determine whether tampering has occurred, and the mobile code, in turn, cannot determine whether the platform is malicious.

VI.B.2.2.d Some New Approaches. Besides the obvious approaches of restricting mobile code to fixed itineraries within a network of trusted platforms, or restricting mobile code to travel only one authenticated hop away from home, a number of novel approaches have been proposed. They include the following ideas.

- Subject the mobile code to state appraisal as a compliment to signed code.
- Require the mobile code to convey proof of safety properties of its code.
- Require the mobile code to maintain a record of the platforms visited.
- Require platforms to maintain execution traces of the mobile code.
- Enable the mobile code to execute encrypted functions safely on a platform.

As with the traditional techniques, the focus of the new approaches is primarily on protecting the mobile code platform from malicious mobile code, rather than the reverse. The last two items, however, on execution traces and computing with encrypted functions, offer some hope for an eventual solution that is effective.

VI.B.2.3 The Future of the Technology. The area of mobile code security is in an immature state. While numerous techniques exist to provide security for mobile code, there is not at present an overall framework that integrates compatible techniques into an effective security model. The traditional host orientation toward security persists, and the focus of protection mechanisms within the mobile code paradigm remains on protecting the host platform. However, emphasis is slowly moving toward developing techniques that are oriented toward protecting the mobile code, a much more difficult problem. Fortunately, there are a number of applications where conventional and emerging security techniques should prove adequate, if applied judiciously.

VI.C Multicast

The term *multicast* refers to sending a message to a group of recipients via a single message, while a *unicast* message is sent only to a single recipient. Multicast protocols transmit these multiple copies only as necessary in the network, rather than sending multiple unicast messages directly from the source node. That is, the message duplication occurs within high-speed network components (i.e., routers) rather than at the slower end terminals. Compared to multiple unicast messages, multicast messages traverse shorter paths and consume significantly fewer network resources as well as reducing the data transmission overhead for the sender.

Most of the recent work on multicast issues has concerned the wired, not wireless, world. Indeed, the network and routing problems may not change significantly between the two transmission paradigms. In some cases, wireless systems simply utilize a different transmission mode on the link into the wired system, and while the problems are similar solutions may need adaptation due to possible variations in bandwidth across the multicast subnetwork. Pure wireless systems need to simulate the structure necessary for the hierarchical systems used in the wired community. Conversely, wired systems simulate a broadcast, while wireless systems perform an actual broadcast with the range permitted by the specific communications technology.

In addition, the security issues differ between the two transmission methods. Multicast groups are defined at network routers, switches, or gateways, so the user has very limited control over the group definition, and must assume that all members of the group receive all messages. Still, routing protocols for wired networks may offer some resistance to interception by unauthorized parties (i.e. those outside the group), but the wireless world offers far less security. In some sense, all wireless transmissions are multicast to “the world.” That is, a wireless transmission may be easily intercepted and read by persons having no relationship to the group.

The term “message” should not be taken to mean only textual data. While large organizations will use multicast technology to communicate familiar e-mail messages with various subgroups, the wireless world will emphasize voice and video transmissions. Multimedia conferencing, cooperative workflow, and even distributed simulation applications will take advantage of multicast capabilities. Simpler applications already exist in cellular group calling schemes and pay-per-view satellite TV transmissions.

VI.C.1 Encryption Solutions for Multicast. In the unicast world, the usual method of implementing message security is through encryption. Wired users may use encryption to enable only a subgroup to actually read a message. Wireless multicast systems require encryption to prevent eavesdroppers. However, most existing encryption techniques are designed for *pairwise* communication and do not scale well when hundreds or even thousands of users must share encrypted information. Areas that need further research include trust issues, key management, encryption algorithms utilizing multiple keys, encryption/decryption processing time, and additional information that must be transmitted (perhaps with every packet). All of these technical security issues are complicated by operational issues including how to change groups, add/delete members, and distribute keys.

Current research offers tradeoffs among these issues. Flat architectures [MU1] distribute an identical key to all members of the group. This is perhaps the most efficient scheme, especially if the keys can be pre-distributed to group members. In flat architectures, if a node is added to a group, the designer is faced with two choices: (1) distribute the same key to the new node, allowing the node to “read” previous messages if those have been saved, or (2) require all nodes to change to a new session key, causing a delay in the transmission. Choice (1) is acceptable for time-dependent applications such as TV broadcast, while choice (2) may be preferred for applications that depend upon the quantity of data, not its timeliness. In flat architectures, the question also arises: “if 1,000 people know a secret key, is it really a secret?”

Store-and-forward or hierarchical schemes [MU2-MU3] are currently the technique of choice for wired networks since they improve the handling of additions and deletions. These schemes may designate some nodes to decrypt the message as sent and then re-encrypt it and forward the message to the next group of nodes with a local, group-specific key. This, of course, causes a delay that is unacceptable for some voice or video applications, but works well for many conventional messaging systems.

A third technique is frequently used for TV broadcasts. In this technique, the session key is encrypted with the public keys of all the members. The message length can increase dramatically for large numbers of subscribers. In existing systems this problem can be alleviated by requiring that all “members” subscribing to a particular package share identical keys. Since the number of packages offered to subscribers is limited, the scheme functions within requirements.

VI.C.2 Opportunities for NIST. Multicast in either a wired or wireless environment involves a tradeoff of network traffic volume, message lengths, delays caused by encryption/decryption, key management techniques, impact of nodes added to or deleted from the network and the amount of trust that may be placed on the nodes. Multicast technology is an attempt to solve the general group communication problem while minimizing network impact. The solution to this problem would provide significant benefits to U.S. industry. As currently designed, security is a critical part of that solution. The issues in this area are mostly technical and well suited for research by NIST scientists. Different applications will require different solutions and continued research will provide continued improvements in these solutions. NIST has a long relationship with many industry groups and therefore is in a unique position to refine the technology for these diverse communities.

VII. Future Wireless Information Technologies

The foregoing sections of this white paper considered specific wireless information technologies for which industry will be making significant investments over the next decade. A number of other wireless information technologies remain the subject of active research. Some these technologies are surveyed in the following subsections.

Significant development is expected in the areas of ad-hoc, adaptive, and asymmetric networks carrying data. In ad-hoc networks, mobile devices can come together to form a spontaneous network. Adaptation refers to the ability of devices and accompanying systems to accommodate the environment, and this includes devices, protocols, and operating systems capable of multiple modes of operation. Asymmetry refers to different upstream and downstream transmission rates, which are dynamically adaptable and which differ from the symmetric fixed provisioning framework of traditional mobile phone networks. Additionally, in the near future, wireless data might possibly see significant growth through Infostations that provide discrete high-speed access in unlicensed bands, rather than through evolving cellular phone networks that are not designed for high speed data and that typically have infrastructure costs due to emphasis on design for ubiquitous service, and that need lengthy standards processes.

VII.A Mobile Ad Hoc Networks (MANETs)

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency response and rescue operations, for disaster relief efforts, and for military networks. Advances in information technology for these important types of situations are envisioned for future wireless communications. Since networks for these scenarios cannot rely on centralized and organized connectivity, such networks are called wireless mobile ad hoc networks (MANETs). A MANET is an autonomous collection of mobile users (nodes) that communicate over relatively bandwidth-constrained, wireless links. Each node is equipped with wireless receivers and transmitters and uses antennas that may be omni-directional, highly directional, or possibly even steerable. Due to nodal mobility, the network topology may change rapidly and unpredictably over time. The network is decentralized, where network organization and message delivery must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. Nodes must also contend with the effects of radio communication, including multi-user interference, multi-path fading, and shadowing effects from terrain and buildings. A MANET may operate in a stand-alone manner, or can be connected to a larger, wired network, such as the Internet.

The design of network protocols for MANETs must account for many complex issues. These networks need efficient distributed algorithms to determine network organization (connectivity), link scheduling, and routing. An efficient approach is to consider routing algorithms in which network connectivity is determined during the process of establishing routes. Message routing in a decentralized environment where network topology fluctuates is not a well-understood problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this is not always true for MANETs. Factors such as power expended, variable wireless link quality, propagation path loss, fading, multi-user interference, and topological changes, become relevant issues. The network should be able to adaptively alter routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks desire to maintain a low probability of detection and a low probability of interception. Hence, nodes prefer to radiate as little power as necessary and to transmit as infrequently as possible. A lapse in any of these requirements may degrade the performance and dependability of the network.

Various protocols for executing routing in a MANET have been recently proposed in the Internet Engineering Task Force (IETF). [M1-M5, M8-M11] Other projects are being pursued for mobile wireless networks, including three projects sponsored by the DARPA Global Mobile Information Systems (GloMo) program. [M6-M7] While these protocols are not designed specifically for MANETs, they may provide enhanced performance and robustness over the MANET routing protocols proposed to the IETF.

The set of applications for MANETs is diverse, ranging from small, static networks, which are constrained by power sources, to large-scale, mobile, highly dynamic networks. For this reason no single routing protocol will likely prove optimal for all scenarios. A given protocol will execute efficiently in those networks whose characteristics are in accord with the mechanisms incorporated into the protocol. However, any effective MANET protocol must efficiently handle several inherent characteristics of MANETs, including the following.

- ***Dynamic topology***: Mobility of nodes leads to unpredictable network topology.
- ***Variable capacity wireless links***: Wireless links are bandwidth-constrained. Moreover, since wireless links have lower capacity than wired links, traffic congestion is typical rather than atypical. However, since a MANET often extends a fixed network, the MANET must provide the same services and meet the traffic

demands as a fixed network. These demands will increase, as multimedia traffic becomes more common.

- ***Power constrained operation***: Power conservation is crucial in mobile wireless systems since these networks typically operate off power-limited sources, which dictate whether a network is operational or not.
- ***Physical security***: Mobile networks are more vulnerable to security threats such as eavesdropping and jamming.

The merit of a routing protocol is judged with performance metrics, both qualitative and quantitative. Desirable qualitative properties for a MANET routing protocol include the following.

- ***Distributed****:* The decentralized nature of a MANET requires that any routing protocol execute using a distributed algorithm.
- ***On demand operation****:* Since a uniform traffic distribution cannot be assumed within the network, the routing algorithm must adapt to the traffic pattern on a demand or need basis, thereby utilizing power and bandwidth resources more efficiently.
- ***Loop-free****:* To ensure proper message delivery and efficient network operation, a routing protocol must be free from routing loops that delay or prevent delivery of data.
- ***Security***: Since MANETs are more vulnerable to security threats, provisions for security must be made, e.g., the application of Internet Protocol (IP) security techniques.
- ***Entering and Departing nodes****:* A routing protocol should be able to quickly adapt to entering or departing nodes in the network, without having to restructure the entire network.
- ***Bi-directional and Unidirectional links****:* Since the condition of a MANET is dynamic, a routing protocol should be able to execute on both bi-directional and unidirectional links.

Irrespective of the application or routing protocol employed, MANET technology can be viewed as improved IP-based networking technology for dynamic, autonomous wireless networks. MANET technology is an upcoming area in future wireless communication. Since MANETs are complex networks and are envisioned for diverse applications, the design of these networks is under continual investigation. The ANTD has assumed an active role in the future evolution of MANET technology by assisting DARPA to evaluate the MANET protocols under development within the IETF. The ANTD is also working with the National Communications System (NCS) on using MANET protocols to support emergency preparedness. In addition, the ANTD is working through the NIST ATP to develop novel routing algorithms for MANETs.

VII.B Infostations. Infostations encompass a new paradigm in wireless information technology where wireless subscribers are assumed to be connected only intermittently but frequently with the communications infrastructure [IS1-IS4]. Contrast this model with the traditional wireless communications architecture that attempts to maintain continuous connectivity between wireless subscribers and the communications infrastructure. The Infostation model assumes that our environment is strewn with various embedded radio transceivers that operate over a limited distance. As subscribers move through this environment, whether on foot, in car, or in train, they encounter periods of increasing and decreasing bandwidth availability. Such a model leads to a range of interesting research in low-power radios, in steerable antennas, in trajectory-based communications protocols that plan the delivery of information in stages as a subscribers moves along points of wireless connectivity, and in geographic routing protocols that attempt to deliver information to subscribers within or moving into a area where the information will prove relevant. When the Infostation model is combined with the existing wired and wireless models of communications, a rich array of services might be offered to end subscribers. The Infostation model has driven some of the research at Rutgers WINLAB. In addition, the HP research laboratory in the UK is also investigating the Infostation model. At the present time, the model remains an interesting idea that could have a large impact on the way we communicate, but only in the distant future.

VII.C High-Speed Free-Space Optical Systems. High-speed free-space optics is an emerging technology, still in its infancy. While free-space optics is a line-of-sight technology that does not enjoy the low attenuation benefits of fiber, it can still support high-speed wireless links over short distances or in environments with few disturbances within the line-of-sight. Two areas in which these technologies are emerging are high-speed local area wireless networks and inter-satellite communications. For 1 to 10Mbps LAN applications, the IEEE 802.11 standard includes the infrared (IR) physical layer specification. This year, new IR based short-range links and LANs capable of speeds up to 155Mps have been announced.

In the domain of space communications, laser inter-satellite links have been of interest recently. Such links can provide speeds of tens of Gbps between GEOS, between LEOS, and for inter-orbit links between GEOS and LEOS. A series of projects sponsored by the European Space Agency is culminating in demonstration and deployment of commercial satellite links next year [FSO1]. For these applications, optical technology promises to offer several advantages over RF in terms of mass, power, system flexibility and cost.

Bell Labs recently announced the demonstration of a 2.5 Gbps optical link transmitted over a range of 1.5 miles without wires [FSO2]. The represents a fourfold improvement over the existing free-space optical links, which can achieve 622 Mbps but at relatively short wavelengths. The improvement was achieved by increasing the power output of new fiber-optic amplifiers by ten times over previously available amplifiers. This power boost enabled the amplifiers to use longer wavelengths, to overcome weather conditions, to send signals further, and to transmit at higher data rates. The previous optical wireless links relied on 800-nanometer light output at 100 milliwatts of power. The Bell Labs demonstration used 1.55-micrometer light output a 10 watts. The light signals were transmitted between a source and receiving telescope. Bell Labs researchers believe that transmission rates of tens of Gpbs should be feasible within a few years. Some applications might include fast deployment of terrestrial high-speed optical networks and high-speed communications with satellites. The satellite communications application seems particularly interesting because the current radio frequencies are becoming quite crowded. Since wireless optical links use point-to-point transmission, interference does not present a problem.

While Bell Labs researchers do not foresee free-space optical transmission as a replacement for fiber optics, because it works only on line of sight and because it is attenuated by snow, rain, and fog, the technology could displace current optical wireless links and could compete with radio and microwave transmission technologies in the campus and urban environments. At present researchers predict that wireless optical links could achieve 99% availability over a few hundred yards, with availability dropping to around 90% as the distance exceeds a mile. As free-space optical systems mature over the next few years, they are likely to find their place in niche markets. The network engineering and protocol aspects both for IR terrestrial links as well as for optical satellite links will be largely similar to those of other high-speed technologies being addressed by ITL. The physical layer issues, including appropriate laser technologies and beam collimation, pointing, and tracking, fall into the general domain of other NIST labs. Overall, we recommend that NIST continue to monitor this technology as it develops over the next few years.

VII.D Networking for Pervasive Computing in Smart Spaces. Increasingly people work and live on the move. To support this mobile lifestyle, especially as work becomes more intensely information-based, companies are producing various portable and embedded information devices. Consider for example, portable digital assistants [PC2], cellular telephones [PC3], the CrossPad [PC4], the InfoPen [PC5], active badges [PC6], intelligent buttons [PC7], and the Internet Car [PC8]. Concurrently, some interesting wireless technologies, including Bluetooth [PCW5], IrDA [PCW15], and HomeRF [PCW6], promise to outfit portable and embedded devices with high bandwidth, localized wireless communication capabilities that can also reach the globally wired Internet. An impressionist painting emerges of small, specialized devices roaming among islands of wireless connectivity within a global ocean of wired networks. Each wireless island becomes a "Smart Space", where available services and embedded devices can be discovered, accessed, interconnected with portable devices carried onto the island, and then the combination of imported and native devices can be exploited to support the information needs of the current island inhabitants. This painting suggests some wonderful potential outcomes, once a number of research and development challenges have been mastered. One key challenge is integration of mobile code technology with pico-cellular wireless technology.

Most people have heard about the Java [PC9] promise of write-once, run-anywhere software. Java makes this possible by requiring Java-compliant systems to implement an interpreter for a Java Virtual Machine (Java VM [PC10]). In fact, a number of initiatives are underway to design chips that run the Java VM in hardware. Additionally, Sun and IBM have been designing an operating system, JavaOS [OS9, OS10, OS13], intended to provide operating services native to Java programs by implementing a small kernel around a JavaChip [PC11]. No matter what the outcome of these explorations, it appears possible to implement the Java VM on a chip (Java or otherwise) with fairly substantial memory and reasonable speed. Combining a Java VM-on-a-chip with a RF transceiver-on-a-chip could provide an interesting basis for networking Smart Spaces devices, especially with the advent of Jini [DAS1].

Jini is a Java-based networking technology recently announced by Sun. Jini enables devices, newly added to a network, to discover a lookup service and to deposit there some key information. This information can include a description of the device and its services, along with Java classes that can be used by others to communicate with the device. In addition, Jini enables programs and devices to discover other devices in an area, and then to download Java code that permits communication with the discovered devices. Along with Jini comes extensions to the Java VM to support event distribution among distributed Java VMs, and extensions to Java Remote Method Invocation (RMI) [PC12] to exploit multicast protocols.

As should now be clear, the ingredients exist to provide Smart Spaces devices with powerful networking functionality in a small, low-power package. Such a package would include a RF transceiver-on-a-chip, a hardware implementation of the Java VM, and enough memory to run the Jini discovery protocols, to hold Java classes for uploading to a Jini lookup service, and to execute Java classes downloaded from a Jini lookup service. Working with DARPA, NIST can provide the technical leadership needed to bring pico-cellular wireless technology together with Jini discovery and lookup services in order provide a suitable networking environment for pervasive computing in Smart Spaces.

VIII. Market Inhibitors

The foregoing material provides some insights into factors that might well inhibit the market success of various wireless communications technologies. This section captures these market inhibitors in the form of tables. Each table addresses one broad area of wireless communications, considering technical, standards, and economic barriers for specific technologies. The broad areas addressed include 3rd Generation Wireless, Broadband Wireless, and Pico-Cell Wireless. Each table is placed on a separate page.

VIII.A 3rd Generation Wireless Market Inhibitors

	Technical Barriers	Standards Barriers	Economic Barriers
3G Terrestrial Systems	➢ Achieving high speed transmission for mobile users in cars or trains ➢ Sufficient frequency spectrum may be unavailable in all countries ➢ Requirement for backward compatibility with a variety of 2G systems ➢ Interconnecting with wired Internet while maintaining suitable quality of service ➢ Providing adequate security services for mobile subscribers	➢ Two, strong warring camps, cdma2000 and W-CDMA ➢ Frequency allocation for IMT-2000 systems varies from country to country ➢ Proposed techniques have traditionally been evaluated solely by the proposer of the technique	➢ Dual-mode or multi-mode phones for backward compatibility with 2G systems could be expensive ➢ Key patents are held by the two main contenders for the standard; this might well lead to an inferior compromise in the specifications included in the standards
3G Satellite Systems	➢ Designing routing and hand over algorithms is complex ➢ Difficult to achieve high speed wireless channels to end users	➢ Standards should not be much of a barrier, though handsets must then be designed specifically for each satellite service provider	➢ Satellite constellations expensive to deploy and maintain ➢ Cost of service might be too high for most subscribers ➢ Countries without fixed telephone infrastructure might be an excellent market, but such countries tend to be poor

VIII.B Broadband Wireless

	Technical Barriers	Standards Barriers	Economic Barriers
MMDS	➢ Downstream bandwidth limited to 1 Gbps, which limits number of simultaneous users unless complex costly sectorization techniques employed ➢ Limited upstream bandwidth vs. downstream bandwidth (6 Mbps vs. 1 Gpbs)		➢ Limited market; leading US supplier, with only 165,000 subscribers, recently de-listed from the NASDAQ ➢ Hard competition from cable and telephony companies (cable modem and xDSL)
LMDS	➢ Requires highly directional antennas ➢ Operates in a difficult frequency band prone to interference from weather ➢ Ill-suited for mobile users ➢ Customer premise equipment must be engineered to cost around $200	➢ Several large companies offer competing proprietary solutions ➢ FCC cedes decisions on spectrum use to operators and equipment suppliers ➢ Spectrum assignments vary around the world ➢ Many standards bodies setting technical LMDS specifications for specific purposes	➢ Uncertain market ➢ As a home access technology, hard competition from cable and telephony companies ➢ Customer premise equipment currently costs about $1,000 ➢ Residential services not expected before 2005
HALO	➢ Relies on existence of LMDS customer premises equipment ➢ Complex to design and deploy ➢ Laser communications with LEOS could prove complex to engineer	➢ Requires permissions from both the FAA and the FCC	➢ Requires 24x7 coverage of populated areas by manned aircraft ➢ Subject to outages if planes crash or suffer maintenance disorders ➢ $40 a month fee for T-1 service might prove too expensive for most potential subscribers
Sky Station	➢ Sky Station user terminals capable of 2-10 Mbps must be designed and built	➢ Requires permissions from both the FAA and the FCC ➢ Down link frequency likely to interfere with radio astronomy	➢ Must deploy multiple Sky Stations at 22 kilometers altitude, with 250 required for maximum coverage
Non-GEO Satellites	➢ Must develop on-board processing units to meet bandwidth, power, and mass requirements for Ka-band ➢ Inter-satellite links difficult to engineer ➢ Require complex tracking and hand over protocols		➢ Expensive to deploy and maintain constellations of earth-orbiting satellites ➢ Uncertain if cost of service will prove attractive to customers ➢ Requires initial investment of billions of dollars
GEO Satellites	➢ Must develop on-board processing units to meet bandwidth, power, and mass requirements for Ka-band		➢ Downlink signals in the 28-30 GHz range might interfere with LMDS operators

VIII.C Pico-Cell Wireless Market Inhibitors

	Technical Barriers	Standards Barriers	Economic Barriers
Wireless LANs	➢ Keeping pace with speed increases seen on wired LANs with which wireless LANs must interconnect ➢ Interference among subscribers as the number of users in a given locale grow ➢ Shrinking size of interface card and antenna	➢ Providing backward compatibility with the IEEE 802.11 standard as the speed of wireless LANs is increased	➢ Per port cost still double the per port cost for 10 Mbps wired LANs
Wire Replacements	➢ Possible ambiguity, incompleteness, and conflict in natural language specification ➢ Untried internetworking of pico-nets ➢ Possible interference from other emitters in the ISM band, including microwave ovens ➢ Need to identify suitable high-level (above link layer) protocols for pico-cellular networks ➢ Need to access capacity of a pico-cellular networks ➢ Need device and service discovery approaches	➢ Need standards for interconnecting pico-nets and for interconnecting pic0-nets networks with the wired Internet ➢ Need to define APIs enabling software to access pico-cellular networks	➢ Transceiver must cost under $5 ➢ Possible competition with wireless LANs, Infrared and with cellular telephone modems

IX. Projections

This section makes some projections about the likely situation over the next decade in three areas of the wireless market: (1) 3rd Generation Wireless Systems, (2) Broadband Wireless Systems, and (3) Pico-Cell Wireless Systems. In addition, the section considers likely progress in a market for Pervasive Computing, which can broadly be viewed as network-based computing where the needed information is available for each user at the right time and place, even as a user switches location and access device. The potential market for pervasive computing technology and services will encompass most of the technologies discussed in this white paper. In fact, pervasive computing will also require technical advances in the area of human-information interaction as well. But that is another story, for another white paper.

IX.A 3rd Generation Wireless Systems

Where will third generation wireless systems be in a decade? There will be at most two global wireless telephony systems based on non-stationary earth orbiting satellites. The number could be as few as zero, depending on the cost of deploying and maintaining satellite constellations, as well as on the difficulty. Can subscribers afford the cost of these services, especially when terrestrial wireless services will be available across most of the world's population? Phrased another way, can the satellite telephony providers bring the cost low enough to compete with terrestrial providers, or can they find a large enough market niche to survive? This seems unlikely, unless governments subsidize such services. Another problem for the satellite-based systems is that the technical capabilities of terrestrial systems will advance to provide multimedia services that satellite-based systems will not be able to match.

Where then can we expect to find the terrestrial 3G services in ten years? Given the demands of wireless telephony operators for backward compatibility with 2G systems, we can expect to find multi-mode handsets capable of working with today's systems as well as with tomorrow's 3G systems. In the best case, the need for multi-mode phones will encompass a transition period lasting only a few years. After that, there will be only 3G systems operating and all the spectrum used for 2G systems transferred to 3G systems. This will, of course, raise the complexity, cost, size, weight, and power consumption of 3G handsets. If one buys a multi-mode phone, then one might be stuck with it or could buy another one later. Still, given the huge investment in 2G infrastructure, no other outcome should be expected. Another effect of this demand for backward compatibility, coupled with the technology fight between Qualcomm and European companies, is that any terrestrial 3G standard that emerges from the IMT-2000 standard is likely to allow at least two incompatible interpretations.

Since a large investment will be required to deploy a supporting infrastructure for 3G wireless systems, the rollout of the technology can be expected to take a number of years. Deployment should not take as much time as the rollout of 2G technology because much of the physical infrastructure, such as towers, can be reused. Another factor will also hamper the rollout of 3G technology. At present, there exists a dearth of applications for 3G wireless systems. Since 2G systems provide voice on a satisfactory basis, the rollout of 3G systems must be accompanied by some significant multimedia applications that will entice subscribers to switch to the new service and to pay the higher price. Will the enticement prove to be Web surfacing on the go? How about video teleconferences on the move? What about remote accesses to digital video cameras showing current conditions at specific locations? Will these applications be provided? If so, will they attract a large subscriber base? Many argue that this lack of a "killer applications" should not be cause for concern, because past experience shows that new applications will emerge once the technology is introduced into the market.

IX.B Broadband Wireless Systems

Where will the broadband wireless systems market be in a decade? Two distinct markets must be considered: (1) the market for broadband satellite systems providing backbone services for Internet traffic and (2) the market for broadband wireless access to end subscriber premises, whether residential or business. Each of these is considered in turn.

Systems such as Teledesic are targeting the market for backbone Internet services, perhaps projecting that the terrestrial capacity for such services will prove insufficient, or that multi-national companies will wish to exploit high bandwidth satellite connectivity to countries with no high bandwidth connections to the global, terrestrial Internet. The first premise seems unlikely. Fiber optic cables are being laid down rapidly in the US. Providing such cables in most of the populated world seems to present little challenge. Certainly, fiber optic cables provide capacity well beyond that offered by high bandwidth satellite constellations. Perhaps in selected situations satellite connections will prove more secure from physical attack than will fiber optic cables. Perhaps Teledesic can compete with geosynchronous satellites by offering high bandwidth channels at a lower propagation delay. Still, the cost, complexity, and risk of designing and deploying systems such as Teledesic appear to be quite challenging. A market might emerge for high bandwidth network access for multi-national corporations that do business in countries without high bandwidth terrestrial channels. Will this market be large enough to sustain Teledesic and its one likely competitor? More likely, some significant government customers will be needed, significant in the sense that the service offered by Teledesic be viewed as a critical national asset.

What, then, can be projected for broadband wireless access to end subscriber premises? MMDS has already essentially failed as a going business prospect in the US market. In addition, the major declared US provider of LMDS service, WMP Communications, plans to offer broadband wireless service initially to large businesses and later to medium size businesses. What is the market niche that this service will grab? No service offering for home users is expected prior to 2005. By that time, the home market is likely to be firmly in the grasp of some combination of cable and telephony companies using digital subscriber lines and cable modems to offer home users bandwidth in the 1-2 Mbps range. Even at this bit rate, the cost is likely to run between $25-$50 per month per home. Of course, satellite-based services, such as the Hughes DirectPC [BWS19], will also be competing for this home market. Can LMDS offer more service at a lower price? It seems unlikely. Where then will be the market for LMDS?

IX.C Pico-Cell Wireless Systems

Pico-cellular wireless systems appear to offer some intriguing possibilities. Among the nearly 4.5 billion computer chips sold each year in the world, approximately 4 billion reside within embedded devices, such as microwave ovens, washing machines, and video cassette players. This trend is expected to accelerate, as computer chips find their way into more embedded devices, sensors, and actuators, and also into a growing number of portable and wearable devices expected to appear on the market over the next decade. To date, these chips, hidden within devices, have been largely inaccessible because no network capabilities have been included. With the advent of pico-cellular wireless technologies, such as Bluetooth and HomeRF, this situation is likely to change. Over the course of time, embedded devices will be able to communication with each other, with their users, and with other computers and services connected to the Internet. These new capabilities should open astounding opportunities for improved automation in the home, office, and factory, as well as among mobile professionals. What other advances might result from this changed situation? Perhaps the age of pervasive computing will at last arrive.

IX.D Pervasive Computing

From a networking perspective, pervasive computing envisions leveraging wireless transceivers embedded in every computer chip, along with gateways that connect wireless islands to the wired Internet, in order to provide users with the ability to access and interact with the right information at the right place and time, using the best available devices, in order to perform useful tasks. To achieve a pervasive computing market, a wide range of technological problems must be solved, and solutions must be integrated from the best research in networking, software, security, and human-information interaction techniques. The possibilities and problems involved with pervasive computing are described in another ITL white paper, but Craig Partridge of BBN Technologies, in a recent IEEE Spectrum opinion piece, [PC1] also describes such a vision.

Partridge envisions a radical change along the edges of the Internet, where the desktop PC will be replaced, or augmented, with clusters of wireless devices. The simplest such clusters will simply replace all the wires connecting your PC, monitor, mouse, keyboard, speakers, and printer. While these devices need not be connected directly to the Internet, Partridge wonders why your speakers can't directly tune in radio broadcasts from the Internet and why your monitor shouldn't be able to access video streams without the need to involve your PC. Partridge goes on to describe a more radical cluster of devices, centered on individuals. As people move through the world, the devices they wear or carry can provide their access portal to networked information, no matter where they roam. Similar visions exist for multi-device communications in the home and in the automobile. The interaction between such groups of embedded devices, which might be called "Smart Spaces", and the devices worn or carried into those spaces by people, could indeed produce a revolution in networking and computing as we conceive of it today. In fact, as Partridge reminds us, if "Smart Highways" ever become real, then the interaction between "Smart Highways", "Smart Cars", and "Smart Body LANs" could provide useful information, grounded in a relevant context at our fingertips on a continuous basis.

X. Recommendations

Wireless information technology will clearly have a large role to play in the information economy of the 21st century. The potential technical agenda is vast, so, while

NIST must take a leadership role in wireless information technology developments, the specific program of work must be carefully considered, and perhaps coordinated closely with other agencies of the Federal Government, as well as with industry. Based on the preceding analysis of the current and future landscape supporting wireless information technology, we offer the following recommendations.

1. NIST should avoid involvement in the technical development of satellite-based communications services, whether for global voice telephony or for augmenting the Internet backbone. These markets will see few players; thus, technical standards should not prove a large barrier. In addition, these markets involve technically complex interactions among a range of technologies in which NIST has relatively little expertise. Finally, enormous investments are required to deploy and maintain these wireless technologies. Since a small number of industry players will bear these risks, the value added by NIST participation is unclear.
2. NIST should avoid involvement in the nascent market for stratospheric wireless communications. Here, the likelihood of market success appears low and the market inhibitors appear to be more economics and regulation than technology and standardization.
3. NIST, in the form of EEEL, has organized stakeholders in the LMDS industry to define technical standards under the auspices of the IEEE 802 technical committee. NIST, in the form of EEEL and ITL, is supporting this standards-setting agenda with a technical testbed, N-WEST, consisting of hardware and software elements distributed between Boulder, Colorado and Gaithersburg, Maryland. While NIST is to be commended for taking on the mantle of leadership in this segment of the wireless industry, we must be aware that the market for LMDS services is likely to falter. For this reason, the development of industry service offerings based on LMDS technology should be monitored closely to ensure that: (1) the emerging technology is finding its way into a healthy market with significant growth potential and (2) that LMDS components being offered for sale comply with the technical standards set by the IEEE. If these conditions do not hold, then NIST should reconsider its activities in LDMS standardization.
4. NIST, in the form of ITL, while a latecomer to the standardization of 3G wireless communication systems, is well positioned to provide independent technical evaluations of the proposed standards. More importantly, the NIST ITL program of work should probably concentrate on identifying and demonstrating advanced multimedia applications, possibly connected with Internet access, in order to help industry create a demand for 3G wireless communications services. Without such advanced applications, the market for 3G wireless is likely to grow very slowly, as the providers of 2G service attempt to maximize the profit from their investments in 2G wireless service for voice.
5. NIST, in the form of ITL and ATP, should develop a program of work to encourage the development of a market for pervasive computing based on wireless transceivers embedded in computer-based devices of all kinds. In addition, NIST should coordinate this program of work with advanced research investments that DARPA seems ready to make in this technology. With DARPA funding research to overcome the hard technical barriers, with ATP and industry sharing the investment in risky but feasible infrastructure technology, and with ITL and EEEL helping industry to set

relevant technical standards and to evaluate proposed technical solutions, the market for pervasive computing technology can grow quite large over the next decade or two.

XI. References

[3GW1] http://rs-comm.com/technology.html

[3GW2] http://www.gsm-pcs.org/

[3GW3] http://www.lucent.dk/wirelessnet/who/

[3GW4] http://www.utdallas.edu/~xu8589/cs6386/index.html

[3GW5] http://www.ece.nwu.edu/~phoel/cdma/

[3GW6] http://www.iht.com/IHT/SUP/021997/gsm05.html

[3GW7] http://www.iss97.org/P-07-01.html

[3GW8] http://gold.itu.int/itudoc/itu-t/icg/imt2000/

[3GW9] W.R. Young. Advanced Mobile Phone Service: Introduction, Background, and Objectives. Bell Systems Technical Journal, vol. 58, pp. 1-14, January 1979.

[3GW10] D.J. Goodman. Wireless Personal Communication Systems. Addison-Wesley, 1997.

[3GW11] T.S. Rappaport. Wireless Communications: Principles & Practice. IEEE Press and Prentice-Hall, 1996.

[3GW12] M. Moulay and M.-B. Pautet. The GSM System for Mobile Communications. Palaiseau, France.

[3GW13] Telecommunications Industries Association. Cellular System Dual-Mode Mobile Station – Base Station Compatibility Standard. Interim Standard 54B, December 1992.

[3GW14] K. Kinoshita, M. Kuramoto, and N. Nakajima. Development of a TDMA Digital Cellular System Based on Japanese Standard. Proceedings of the 41st IEEE Vehicular Technology Conference, pp. 642-645, 1991.

[3GW15] C.E. Cook, F.W. Ellersick, L.B. Milstein, and D.L. Schilling. Spread-Spectrum Communications. IEEE Press, 1983.

[3GW16] A.J. Viterbi. CDMA: Principles of Spread Spectrum Communications. Addison-Wesley, 1995.

[3GW17] Telecommunications Industries Association.Mobile Station – Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System. Interim Standard 95, July 1993.

[3GW18] Telecommunications Industries Association.800 MHz TDMA Cellular Radio Interface Mobile Station - Base Station Compatibility. Interim Standard 136A, October 1996.

[3GW19] IEEE Communications Magazine. September 1998.

[3GW20] IEEE Personal Communications Magazine. December 1998.

[3GW21] International Telecommunication Union, Radiocommunication Study Groups. IMT-2000, Report of the 15th Meeting of ITU-R Task Group 8/1, Jersey, Channel Islands, November 1998.

[3GW22] J. Allnutt and B. Woerner. Mobile Satellite Systems. Proceedings of the 10th Federal Wireless Users Forum Workshop. Las Vegas, Nevada, December 1998.

[BWS1] http://nwest.nist.gov/

[BWS2] http://www.wcai.com/How_It_Works.htm

[BWS3] www.fcc.gov/Bureaus/Mass_Media/News_Releases/1998/nrmm8030.html

[BWS4] http://www.itscorp.com/tech/expforum.html

[BWS5] http://www.itscorp.com/tech/a2wayv12.html
[BWS6] http://www.nortel.ca/wireless/bwa/ptmp.html
[BWS7] http://www.davic.org/
[BWS8] http://www.etsi.org/
[BWS9] http://www.etsi.org/bran/bran.htm/
[BWS10] http://www.umts-forum.org/
[BWS11] http://www.de.infowin.org/ACTS/
[BWS12] http://www.uk.infowin.org/ACTS/RUS/PROJECTS/ac215.htm
[BWS13] http://www.angeltechnologies.com/
[BWS14] http://www.skystation.com/
[BWS15] http://www.skystation.com/service.html
[BWS16] http://www.spotbeam.com/mansum.htm
[BWS17] http://www.teledesic.com/
[BWS18] http://www.skybridgesatellite.com/
[BWS19] http://www.primefocus.com/directpc.html
[BWS20] Fred Langa, "High-Speed Surfing", *Windows Magazine*, February 1999, page 166.
[BWS21] Fred Langa, "High-Speed Surfing", *Windows Magazine*, February 1999, page 166.
[DAS1] http://www.sun.com/jini/
[DAS2] http://www.srvloc.org/intro.html
[FSO] http://esapub.esrin.esa.it
[IS1] http://www.cs.rutgers.edu/~badri/dataman/nimble
[IS2] http://www.cs.rutgers.edu/~katsaros/ISintro/index.htm
[IS3] http://winwww.rutgers.edu/pub/projects/Spring98/p002.html
[IS4] http://hubub.epri.com/csg/ist/wso/wsodeliv/index.html
[M1] Z.J. Haas and M. R. Pearlman. The Zone Routing Protocol (ZRP) for Ad Hoc Networks. Internet Draft, Nov. 1997.
[M2] C. Perkins and E.M. Royer. Ad Hoc on Demand Distance Vector (AODV) Routing. Internet Draft, Aug. 1998.
[M3] V.Park and S.Corson. Temporally-Ordered Routing Algorithm (TORA). Internet Draft, Aug. 1998.
[M4] J.Broch, D.B.Johnson, and D.A.Maltz. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. Internet Draft, Mar. 1998.
[M5] M. Jiang, J.Li, and Y.C. Tay. Cluster Based Routing Protocol (CBRP) Functional Specification. Internet Draft, Aug. 1998.
[M6] J.J. Garcia-Luna-Aceves, C.L. Fullmer, E. Madruga, D. Beyer, and T. Frivold. Wireless Internet Gateways (WINGS). In Proc. IEEE MILCOM, Monterey, CA, Nov. 1997.
[M7] S. Ramanathan and M. Steenstrup. Hierarchically-organized, multihop mobile networks for multimedia. ACM/Baltzer Mobile Networks and Applications, 3(1):101--119, 1997.
[M8] Bommaiah, McAuley, Talpade, and Liu. Ad Hoc Multicast Routing Protocol. Internet Draft, Aug. 1998.
[M9] R.Sivakumar, P.Sinha, and V.Bharghavan. Core Extraction Distributed Ad Hoc Routing (CEDAR) Specification. Internet Draft, Oct. 1998.

[M10] M.Gerla, G.Pei, S.Lee, and C.Chiang. On-Demand Multicast Routing Protocol (ODMRP) for Ad-Hoc Networks. Internet Draft, Nov. 1998.

[M11] P.Jacquet, P.Muhlethaler, and A.Qayyum. Optimized Link State Routing Procotol. Internet Draft, Nov. 1998.

[MC0] "Mobile Agents White Paper," General Magic, 1998 http://www.genmagic.com/technology/techwhitepaper.html

[MC1] A. Fuggetta, G.P. Picco, and G. Vigna, "Understanding Code Mobility," IEEE Transactions on Software Engineering, 24(5), May 1988 http://www.cs.ucsb.edu/~vigna/listpub.html

[MC2] James Gosling and Henry McGilton, "The Java Language Environment: A White Paper," Sun Microsystems, May 1996 http://java.sun.cm/docs/white/langenv/

[MC3] Danny Lange and Mitsuru Oshima, Programming and Deploying Java Mobile Agents with Aglets,Addison-Wesley, 1998

[MC4] Anurag Acharya, M. Ranganathan, Joel Salz, "Sumatra: A Language for Resource-aware Mobile Programs," in J. Vitek and C. Tschudin (Eds.), Mobile Object Systems: Towards the Programmable Internet, Springer-Verlag, Lecture Notes in Computer Science No. 1222, pp. 111-130, April 1997 http://www.cs.umd.edu/~acha/papers/lncs97-1.html

[MC5] "Agent Management," FIPA '97 Specification, part 1, version 2.0, Foundation for Intelligent Physical Agents, October 1998 http://www.fipa.ord/spec/fipa97/fipa97.html

[MC6] "Mobile Agent System Interoperability Facilities Specification," Object Management Group (OMG) Technical Committee (TC) Document orbos/97-10-05, November 1997 http://www.omg.org/techprocess/meetings/schedule/Technology_Adoptions.html

[MC7] William Farmer, Joshua Guttman, and Vipin Swarup, "Security for Mobile Agents: Issues and Requirements," Proceedings of the 19th National Information Systems Security Conference, Baltimore, MD, pp. 591-597, October 1996 http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper033/

[MC8] Markus Straßer, Joachim Baumann, Fritz Hohl, "Mole - A Java Based Mobile Agent System," in M. Mühlhäuser (ed.), Special Issues in Object Oriented Programming, Verlag, 1997, pp. 301-308 http://www.informatik.uni-stuttgart.de/ipvr/vs/projekte/mole/ECOOP96.ps.gz

[MC9] "ObjectSpace Voyager Core Package Technical Overview," version 1.0, ObjectSpace Inc., December 1997 http://www.objectspace.com/developers/voyager/white/index.html

[MC10] Joseph Tardo and Luis Valente, "Mobile Agent Security and Telescript," Proceedings of IEEE COMPCON '96, Santa Clara, California, pp. 58-63, February 1996, IEEE Computer Society Press

[MC11] Robert S. Gray, "Agent Tcl: A Flexible and Secure Mobile-Agent System," Proceedings of the Fourth Annual Tcl/Tk Workshop (TCL 96), pp. 9-23, July 1996 http://actcomm.dartmouth.edu/papers/#security

[MC12] John K. Ousterhout, Jacob Y. Levy, and Brent B. Welch, "The Safe-TCL Security Model," Technical Report SMLI TR-97-60, Sun Microsystems, 1997

[MC13] Li Gong, “Java Security Architecture (JDK 1.2),” Draft Document, revision 0.8, Sun Microsystems, March 1998 http://pcba10.ba.infn.it/api/jdk1.2beta3/docs/guide/security/spec/security-spec.doc.html

[MC14] Günter Karjoth, Danny B. Lange, and Mitsuru Oshima, "A Security Model For Aglets," IEEE Internet Computing, August 1997, pp. 68-77

[MC15] “Odyssey Information,” General Magic Inc., 1998 http://www.genmagic.com/technology/odyssey.html

[MC16] William Farmer, Joshua Guttman, and Vipin Swarup, “Security for Mobile Agents: Authentication and State Appraisal,” Proceedings of the 4th European Symposium on Research in Computer Security (ESORICS '96), September 1996, pp.118-130

[MC17] G. Necula and P.Lee, "Safe Kernel Extensions Without Run-Time Checking," Proceedings of the 2nd Symposium on Operating System Design and Implementation (OSDI '96), Seattle, Washington, October 1996, pp.229-243 http://www.cs.cmu.edu/~necula/papers.html

[MC18] Giovanni Vigna, "Protecting Mobile Agents through Tracing," Proceedings of the 3rd ECOOP Workshop on Mobile Object Systems, Jyvälskylä, Finland, June 1997 http://www.cs.ucsb.edu/~vigna/listpub.html

[MC19] Volker Roth, “Secure Recording of Itineraries through Cooperating Agents,” Proceedings of the ECOOP Workshop on Distributed Object Security and 4th Workshop on Mobile Object Systems: Secure Internet Mobile Computations, pp. 147-154, INRIA, France, 1998 http://www.igd.fhg.de/www/igd-a8/pub/#Mobile%20Agents

[MC20] Joann J. Ordille, “When Agents Roam, Who Can You Trust?” Proceedings of the First Conference on Emerging Technologies and Applications in Communications, Portland, OR, May 1996 http://cm.bell-labs.com/cm/cs/doc/96/5-09.ps.gz

[MC21] Thomas Sander and Christian Tshudin, ”Protecting Mobile Agents Against Malicious Hosts,” in G. Vinga (Ed.), Mobile Agents and Security, Springer-Verlag, Lecture Notes in Computer Science No.1419, 1998 http://www.icsi.berkeley.edu/~tschudin

[MU1] G. Caronni, H.Lubich, A.Aziz, T. Markson, R. Skrenta, “Skip: Securing the Internet”, *proceedings: IEEE Fifth Workshop on Enabling Technologies (WET ICE)*, 1996.

[MU2] K.P. Kihlstrom, L.E. Moser, P.M. Melliar-Smith, “the SecureRing Protocols for Securing Group Communication”, *proceedings: IEEE 31st Hawaii International Conference on System Sciences*, Kona, HI, Jan. 1998, vol.3, pp. 317-326.

[MU3] D.M. Wallner, E.J. Harder, R.C. Agee, “Key Management for Multicast: Issues and Architectures”, *Internet Working Group Draft*, September 1998.

[OS1] George Lawton, "Vendors Battle over Mobile-OS Market", *Computer*, February 1999, pp. 13-15.

[OS2] http://www.geoworks.com/

[OS3] Marcus Groeber, "Nokia 9000 SDK: A (GEOS) Developer's Perspective", *Handheld* Systems, May/June 1997.

[OS4] http://www.palm.com/newspromo/corporate/platform.html

[OS5] Palm Computing, "The Palm Operating System - Technology Overview", *PDA Developers*, March/April 1996.

[OS6] http://www.microsoft.com/windowsce/default.asp

[OS7] Steve Mann, "Windows CE Developer's Overview", *PDA Developers*, November/December 1996.

[OS8] John Schettino, "Getting Up To Speed With Windows CE", *Handheld Systems*, May/June 1997.

[OS9] Peter W. Madany, "JavaOS: A Stand-Alone Java Environment", *PDA Developers*, July/August 1996.

[OS10] http://java.sun.com/products/javaos/index.html

[OS11] http://www.zdnet.com.au/zdimag/news/199703/06/news2.html

[OS12] http://www5.zdnet.com/zdnn/content/pcwo/03060012.html

[OS13] http://java.sun.com/products/javaos/javaos.white.html

[PC1] Craig Partridge, "Viewpoint: Embedded wireless connects Net to all and all to Net", *IEEE Spectrum*, January 1999, page 38.

[PC2] http://www.pdapage.com/

[PC3] http://www.portableconcepts.com/

[PC4] http://www.crosspad.com/

[PC5] http://www.symbol.com/data/std00055.htm

[PC6] http://www.ics.agh.edu.pl/ABng/

[PC7] http://www.ibutton.com/

[PC8] http://www.daimler-benz.com/ind_gfnav_e.html?/research/text/70430_e.htm

[PC9] http://www.sun.com/java/

[PC10] http://java.sun.com/docs/books/vmspec/

[PC11] http://www.sun.com/microelectronics/picoJava/index.html

[PC12] http://java.sun.com/products/jdk/rmi/

[PCW1] http://www.newsbytes.com/pubNews/88/48985.html

[PCW2] http://www.etsi.fr/dect/dect.htm

[PCW3] http://www.etisalat.co.ae/s_gsm.htm

[PCW4] http://www.rangelan2.com/learn/whiteppr/80211wp.shtml

[PCW5] http://www.bluetooth.com

[PCW6] http://www.homerf.org

[PCW7] http://www.uplanet.com/

[PCW8] http://www.cnp-wireless.com/PCS.html

[PCW9] http://w3.antd.nist.gov/~mills/whitepapers/airjava_sans$_.pdf

[PCW10] http://grouper.ieee.org/groups/802/11/index.html

[PCW11] http://www.ericsson.se/Review/er3_98/art1/art1.html

[PCW12] http://www.gsmdata.com/artblue.htm

[PCW13] Pat Megowan, "IR Reflections", *PDA Developers*, July/August 1996.

[PCW14] Pat Megowan, "IR Relections", PDA Developers, January/February 1997.

[PCW 15] http://www.irda.org

[WCS1] G. Pierce and C. Paar, "Recent Developments in Digital Wireless Network Security", Conference on Telecommunications Research and Development in Massachusetts, Worcester Polytechnic Institute, March 1996.

[WCS2] "Current and Future Functional Requirements for Federal Wireless Services in the United States", Federal Wireless Policy Committee, November 1998. http://www.antd.nist.gov/~ruhl/reqsdocr11.html,

[WCS3] Bruce Schneier, "Applied Cryptography, Protocols, Algorithms, and Source Code in C", Second Edition, Wiley & Sons, 1996.

[WCS4] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", Internet Society, IETF RFC 2401, November 1998.

[WCS5] John Scourias, "Overview of the Global System for Mobile Communications", University of Waterloo, Ontario, Canada, October 1997. http://www.gsmdata.com/overview.htm,

[WCS6] D. Maughan, M. Schertler, M. Schneider, J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", Internet Society, IETF RFC 2408, November 1998.